

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 907 120 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.04.1999 Bulletin 1999/14

(51) Int. Cl.⁶: G06F 1/00, H04L 9/32

(21) Application number: 98118486.4

(22) Date of filing: 30.09.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 02.10.1997 US 957986
09.04.1998 US 57966

(71) Applicant:
Tumbleweed Software Corporation
Redwood City, California 94063 (US)

(72) Inventors:
• Smith, Jeffrey C.
Menlo Park, CA 94025 (US)
• Bandini, Jean-Christophe
Cupertino, CA 95014 (US)
• Shoup, Randy
San Francisco, CA (US)

(74) Representative:
Diehl, Hermann, Dr. Dipl.-Phys. et al
DIEHL, GLÄSER, HILTL & PARTNER
Patentanwälte
Augustenstrasse 46
80333 München (DE)

(54) Method and apparatus for delivering documents over an electronic network

(57) A method and apparatus are provided for securely delivering documents over an electronic network (18) while preserving document formatting. The invention also provides security that restricts access to the system to an authorized user. A document is sent from a sending computer (14) to a dedicated server (22), using a send client application (20). A dedicated server (22) stores the document (16) and forwards an electronic notification to a receiving device (24,26,28). The stored document is downloaded from the dedicated

server (22), using a receive client application (30), in response to the notification. The receive client application (30) permits the recipient to receive, view, print, and/or manipulate the document. A sender driven certificate enrollment system (1342) and methods of its use are also provided, in which a sender (1352) controls the generation of a digital certificate (1345) that is used to encrypt and send a document to a recipient (1370) in a secure manner.

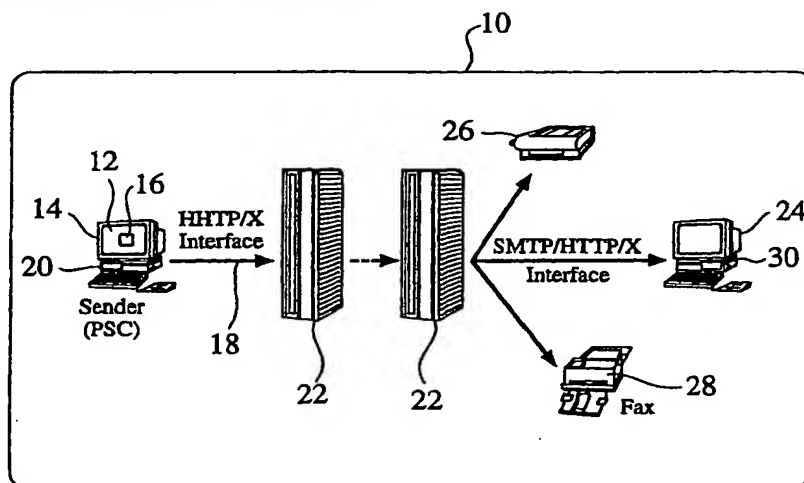


Fig. 5

Description

[0001] The invention relates to communication over an electronic network. The invention relates to a method and apparatus for delivering formatted documents over an electronic network, such as the Internet, in a secure fashion. Further, the invention relates to the field of electronic document encryption. More particularly, the invention relates to techniques for the secure delivery of electronic documents to remote recipients.

[0002] Electronic networks, such as the Internet and intranets are increasingly being used to store and distribute a variety of data. For example, a World Wide Web (Web) page may include text, graphical displays, video displays, animation, and sounds. The Web enables a recipient to receive a document from a sender, regardless of platform, operating system, or E-mail system. Such communication is possible even when the document is not received at a computer but, rather, is received at a fax machine or networked printer connected to the Internet.

[0003] In many instances, the sender of a document resides on a local area network, referred to herein as an intranet. The sender's computer may be connected to the Internet directly, or through the intranet's server. Users who do not have a direct Internet connection can subscribe to the services of an access provider, called an Internet Service Provider (ISP) in the case of the Internet.

[0004] The ISP maintains a network that connects its clients to the Internet, providing a server computer that acts as a host to its clients. The client accesses the Internet by using a computer with a modem to dial up the ISP, through the public telephone system. The ISP usually provides a point-to-point (serial) link through which the client communicates directly to the Internet, using the Internet standard TCP/IP protocols.

[0005] Existing transmission schemes are frequently not suitable for sending certain documents over, for example, the Internet. Critical documents must be sent with complete security. However, the disparate E-mail systems have varying levels of security support. It is therefore difficult or impossible to determine whether an electronic communication is secure.

[0006] Various cryptographic schemes have been used to provide security for electronic communications. However, the recipient of an encrypted message must have not only the decryption scheme, but sufficient hardware and software to decrypt the communication. Thus, it is frequently not practical or possible to send such an encrypted message.

[0007] Thus, users are often reluctant to send documents electronically. These users must rely upon the slower and more expensive methods of courier service, and conventional mail service.

[0008] It is also desirable to be able to track a critical or sensitive document to insure that it has been properly received. However, it is extremely difficult, if not impos-

sible, to track a document from point to point along the electronic network. For example, an E-mail message sent via the Internet is broken up into many discrete data packets. The packets are sent separately through the Internet to the intended recipient. Each packet may take a different route before being re joined to form the original document and delivered to the recipient. Therefore, tracking such document has required tracking each individual packet through each link of the Internet.

[0009] Additionally, while a computer may provide some level of security for a received document, for example, with passwords or cryptography, an electronic communication is not necessarily directed to a computer. Thus, a critical document sent electronically to a printer or a fax machine is potentially exposed to public view.

[0010] Even if such document is transmitted securely, it may not be legible when received. One problem common to E-mail is loss of document formatting. A document sent via E-mail is typically sent either as text in the body of the E-mail message, or as an attachment thereto. A text document usually does not retain the formatting of the original document. An attached document can retain formatting in some circumstances, such as if both sender and recipient have compatible software applications. However, some formatting may be lost even when the recipient opens a received document using the same application in which it was created.

[0011] Changes in document formatting can create significant problems. Electronic forms may not be compatible if their formats are different. A misformatted document may not be comprehensible to the recipient. While many formatting changes are correctable, the costs to the recipient in terms of time and expense may be substantial.

[0012] It is therefore an advantage to provide a method and apparatus for securely delivering documents over an electronic network, such as the Internet. It is a further advantage if such method and apparatus tracks the sending and receipt of a document. It is yet another advantage if such method and apparatus preserves the formatting of a delivered document.

[0013] The development of computerized information sources, such as those provided through the Internet or other on-line sources, has led to a proliferation of electronically available information. The desired or required security for the secure distribution of information and documents across networks has led to a variety of architectures and techniques to protect this information.

[0014] Encryption is a basic technique to scramble information or documents to prevent unsolicited access to that information.

[0015] Figure 1 is a block diagram of secret key encryption 1210a, wherein a document 1212 is encrypted, or scrambled 1216, with a secret key 1214, producing an encrypted document 1220. The encrypted document 1220 can then be transferred to a recipient.

Secret key encryption, sometimes referred to as symmetric key cryptography, employs a technique of scrambling information to prevent unsolicited access, using a unique, secret key 1214.

[0016] Figure 2 is a block diagram of secret key decryption 1210b, wherein the same, unique secret key 1214 is required to unscramble 1222 the encrypted document 1220, to reproduce a copy of the original document 1212. Without access to the secret key 1214, an encrypted document 1220 remains secure from tampering.

[0017] One potential issue with secret key encryption 1210a and 1210b is the challenge of distributing the secret key 1214 securely. For example, suppose a sender uses secret key encryption to encrypt a document 1212, and then sends a recipient the encrypted document 1220. The recipient needs the secret key 1214 to decrypt 1222 the encrypted document 1220. If the secret key 1222 is sent over a non-secure channel, then the integrity of the security is compromised. For most applications, telephone or fax provides a secure enough means of delivering secret keys 1214, while the encrypted document 1220 can be delivered over the internet using the Posta™ document delivery system. In some instances, however, senders and recipients require a more robust or convenient means of distributing a secret key 1214.

[0018] Public key encryption facilitates a more robust, and typically a more convenient means, of delivering information securely. With public key encryption, each recipient owns a pair of keys, called a public key and a private key. The key pair's owner (the recipient) publishes the public key, and keeps the private key a secret.

[0019] Fig. 3 is a block diagram of public key encryption 1230a, wherein a document 1312 is encrypted, or scrambled 1234, with a public key 1332, producing an encrypted document 1336. To send information to a recipient, a sender uses the published public key 1332 of the intended recipient to encrypt 1234 the information, and then the recipient uses their own private key 1334 (Fig. 4) to decrypt the information. Hence, the private key 1334 (which is necessary to decrypt the information) is not distributed. Fig. 4 is a block diagram of private key decryption 1230b, wherein the private key 1334 is required to unscramble 1238 the encrypted document 1336, to reproduce a copy of the original document 1312. Without access to the private key 1334, an encrypted document 1336 remains secure from tampering.

[0020] Public key encryption 1230a and 1230b typically exploits a mathematical relationship between the public and private keys 1332, 1334, which allows a public key 1332 to be published, without risking the derivation of the private key 1334 from the published public key 1332.

[0021] Public key encryption algorithms are typically complex, and hence may be too time consuming to be of practical use for many users. Secret key encryption

1210a, 1210b is typically much faster than public key encryption 1230a, 1230b, but requires the transmission the secret key 1214 from the sender to the recipient.

[0022] In a digital envelope system, a user encrypts a document 1212 with a secret key 1214, and then encrypts the secret key 1214 with the public key 1332 of the intended recipient. The recipient of the encrypted document 1220 then uses their private key 1240 to decrypt the secret key 1214, and then uses the secret key 1214 to decrypt the document.

[0023] It is often useful to verify if a document has not been altered during transmission, or to verify who sent or received a given document. Hashing algorithms (or message digests) and public key technologies facilitate solutions to document integrity and transport verification.

[0024] Digital certificates can also be used to provide enhanced security for encrypted information. Suppose a recipient owns a public/private key pair and wishes to publish the public key 1332 so others can use the public key 1332, either to encrypt information to be sent to the recipient, or to verify the digital signature of the recipient. A secure technique for the recipient to publish the public key 1332 is to register the public key 1332 with a trusted authority. The trusted authority can then certify that a particular public key 1332 belongs to the recipient. A digital certificate connects a recipient, or other entity, with a particular public key 1332.

[0025] A digital certificate, as disclosed later, is a record of a public key and an identity, and the association of the two as attested to by a third party by means of a digital signature. The private key is not in the certificate, but only one private key can match a given public key. A public/private key pair is actually a pair of numbers with the following properties.

- The private key cannot be derived easily from the public key; and
- The public key can be used to cipher data which can only be deciphered by knowing the private key (some public keys algorithms, such as RSA, also have the inverse property, which makes them suitable for use a digital signatures).

[0026] A trusted or certificate authority issues and maintains digital certificates.

[0027] The disclosed prior art systems and methodologies thus provide some methods for the encryption and secure delivery of documents, but fail to provide a simple digital certificate generation and enrollment system that is implemented and controlled by a sender. The development of such a digital certificate system would constitute a major technological advance.

[0028] It is therefore the object of the present invention to provide an apparatus for managing and delivering documents, which overcomes the drawbacks of the prior art. This object is solved by the apparatus for man-

aging and delivering documents according to independent claims 1 to 10 and the apparatus for generating a digital certificate according to independent claim 23, as well as the method for document management and delivery according to independent claim 16 and the method for generating a digital certificate according to independent claim 34. Further advantageous features, aspects and details of the invention are evident from the dependent claims, the description and the drawings. The claims are to be understood as a first non-limiting approach to define the invention in general terms. The invention relates to a method and apparatus for delivering formatted documents over an electronic network, such as the Internet, in a secure fashion. Further, the invention relates to the field of electronic document encryption. More particularly, the invention relates to techniques for the secure delivery of electronic documents to remote recipients. It is therefore an advantage to provide a method and apparatus for securely delivering documents over an electronic network, such as the Internet. It is a further advantage if such method and apparatus tracks the sending and receipt of a document. It is yet another advantage if such method and apparatus preserves the formatting of a delivered document.

[0029] The invention provides a method and apparatus for securely delivering documents over an electronic network. The invention permits a user to track the sending and receipt of a document, while the document's original formatting throughout the delivery is preserved.

[0030] For the purposes of the discussion herein, the term "document" includes any contiguous collection of data, including a stream of data, video data, audio data, animation, a platform-independent formatted document such as an HTML, PDF, or Envoy document, a platform-specific formatted document such as a Microsoft Word or Excel document, an unformatted document such as a text document, a custom-generated report or Web page, or a grouping of one or more database records, such as SQL records. The term document can also include a grouping of one or more such documents. While the preferred embodiment of the invention is adapted for use in document transmission over the Internet, the invention is equally applicable to other wide area or local area networks.

[0031] In accordance with a presently preferred embodiment of the invention, a send client application is provided that allows a user to send a document over an electronic network from the desktop of a sending computer. Such document may also be sent from within a document authoring application.

[0032] A dedicated server is provided to store the document received from the sending computer. The dedicated server then forwards an electronic message to a receiving device to notify the recipient of the document's transmission.

[0033] The intended recipient downloads the stored document from the dedicated server in response to this

message. In the preferred embodiment of the invention, the receiving device is a personal computer. However, in alternate embodiments, the receiving device includes a network server device, fax machine, printer, Internet-compatible telephone, Internet access appliance, or personal digital assistant.

[0034] A receive client application provided on the receiving device is used to download the document from the dedicated server. The receive client application is preferably a Web browser, but can be any other software application capable of retrieving the stored document while preserving document formatting. The receive client application permits the recipient to receive, view, print, and manipulate the document.

[0035] The send client application is accessed via an application window. The application window is displayed on the sending computer's desktop. The application window includes a persistent tool bar for accessing main functions and a menu listing operational commands for the send client application.

[0036] A package manager and a package window are also accessed from the application window. The package manager lists all document activities initiated during an application session. The package window allows the user to specify parameters of the document delivery, including the recipient(s), the document(s), and send options. Document delivery parameters may be stored in a storage module for later modification and/or use.

[0037] A document is specified for delivery in several ways. The user can click and drag the document from the sending computer desktop onto one of the application window or the package window. The document may also be dragged onto either the icon representing the send client application or the icon for accessing the stored document delivery parameters. The user can also browse local and network directories and select desired documents. A document can also be sent from within a document authoring application.

[0038] A configuration user interface (CUI) is provided for directly invoking and customizing the dedicated server. In the preferred embodiment of the invention, the CUI is an HTML interface. The dedicated server is therefore directly invoked and customized via a Web browser. This HTML interface includes modules for sending and tracking the document, accessing account information, managing billings, and managing mail distribution lists.

[0039] The CUI is accessed via a CUI application window displayed on a managing computer desktop. The managing computer can be the sending computer, the receiving computer, the dedicated server, or some other entity in the electronic network. The CUI application window displays a main tool bar for accessing main functions, and a secondary tool bar for accessing secondary functions. The CUI application window also includes a workspace for displaying an interactive interface to an accessed function, and a menu listing opera-

tional commands.

[0040] The invention also provides a security framework that restricts system access to an authorized user. The types of security supported include authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication. The security framework can be implemented as one or more modules, and can be incorporated into at least one of the send client application, the receive client application, and the CUI.

[0041] A sender driven certificate enrollment system and methods of its use are provided, in which a sender controls the generation of a digital certificate, which can be used to encrypt and send a document to a recipient in a secure manner. The sender compares previously stored recipient information to gathered information from the recipient. If the information matches, the sender transfers key generation software to the recipient, which produces the digital certificate, comprising a public and private key pair. The sender can then use the public key to encrypt and send the document to the recipient, wherein the recipient can use the matching private key to decrypt the document. In a preferred embodiment, a server is interposed between the sender and the recipient, to provide increased levels of system security, automation, and integrity.

[0042] The above mentioned and other features of the present invention and the invention itself will be understood by the reference to the following detailed description of the preferred embodiments of the invention, when considered in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram of secret key encryption of a document;

Fig. 2 is a block diagram of secret key decryption of a document;

Fig. 3 is a block diagram of public key encryption of a document;

Fig. 4 is a block diagram of private key decryption of a document;

Fig. 5 is a diagram of a document delivery system according to the invention;

Fig. 6 is a view of an application window according to the invention;

Fig. 7 is a view of an application window showing document activities according to the invention;

Fig. 8 is a view of a package window, according to the preferred embodiment of the invention;

Fig. 9 is a view of a recipient's window according to

the invention;

Fig. 10 is a view of a CUI application window according to the invention;

Fig. 11 is a view of a CUI package window according to the invention;

Fig. 12 is a view of a CUI options page according to the invention;

Fig. 13 is a view of a CUI tracking search page according to the invention;

Fig. 14 is a view of a CUI tracking report preferences dialog according to the invention;

Fig. 15 is a view of a recipient summary tracking report in basic format according to the invention;

Fig. 16 is a view of a recipient detail tracking report in Basic Format according to the invention;

Fig. 17 is a view of a recipient detail tracking report in billing code format according to the invention;

Fig. 18 is a view of a group account manager account - view members window according to the invention;

Fig. 19 is a view of a billing codes window according to the invention;

Fig. 20 is a view of an edit billing codes dialog according to the invention;

Fig. 21 is a view of an add billing codes dialog according to the invention;

Fig. 22 is a view of a create invoice page, according to the invention;

Fig. 23 is a view of a basic invoice report window according to the invention;

Fig. 24 is a view of a billing preferences dialog according to the invention;

Fig. 25 is a view of an invoice report in spec invoice format according to the invention;

Fig. 26 is a view of an invoice report in billing code invoice format according to the invention;

Fig. 27 is a view of a mail list page according to the invention;

Fig. 28 is a view of a mail list detail page according

to the invention;

Fig. 29 is a view of an add addresses page according to the invention; and

Fig. 30 is a flow chart of the method for delivering a document over an electronic network according to the invention.

Fig. 31 shows a basic certificate enrollment system implemented between a sending computer and a receiving computer across a network;

Fig. 32 shows a certificate enrollment system implemented between a sending computer, a SDCE server and a receiving computer;

Fig. 33 shows a certificate enrollment system implemented between a sending computer, a SDCE server, a database server and a receiving computer;

Fig. 34 shows a certificate enrollment system implemented between a sending computer, a SDCE server, a database server, a certificate server and a receiving computer;

Fig. 35 is a block diagram of a digital certificate;

Fig. 36 is a block diagram of a certificate digest;

Fig. 37 shows the first stage of operation for the sender driven certificate enrollment system;

Fig. 38 shows the second, attestation conversation stage of the sender driven certificate enrollment system;

Fig. 39 shows the third, public/private key pair generation stage of the sender driven certificate enrollment system;

Fig. 40 shows the fourth stage of the sender driven certificate enrollment system, referred to as forwarding and registration of the receiver public key; and

Fig. 41 is flow chart that shows the basic decision tree for the sender driven certificate enrollment system.

[0043] The display screens and configuration of the graphical user interface described below are provided in accordance with the presently preferred embodiment of the invention. However, one skilled in the art will appreciate that such display screens and graphical user interfaces are readily modified to meet the requirements of alternative embodiments of the invention. The following

discussion is therefore provided for purposes of example and not as a limitation on the scope of the invention.

[0044] Fig. 5 is a diagram of a document delivery system 10 according to the invention. The system allows the user to send a document 16 or set of documents and a recipient address or set of recipient addresses from the desktop 12 of a sending computer 14 over an electronic network 18 using a send client application 20. Such document may also be sent from within a document authoring application, such as a word processor spreadsheet, or graphics application. The send client application is preferably stored on the sending computer, but may be stored in a remote location accessible to the sending computer.

[0045] The sending computer connects to a dedicated server 22. The dedicated server functions in accordance with such standards as, for example Internet standards to manage the transfer of documents between senders and recipients. The dedicated server may be a server provided by an Internet service provider (ISP), or may be a separate dedicated server.

[0046] In the preferred embodiment of the invention, documents are uploaded to, and downloaded from the dedicated server using the hypertext transport protocol (HTTP). HTTP is the communications protocol used to connect to servers on the World Wide ("Web"). A significant advantage of HTTP is that it is application and platform-independent. Thus, the sender and recipient do not need to use the same Web browser, or even the same operating system.

[0047] The dedicated server 22 stores the document received from the sending computer 14. The dedicated server then forwards an electronic message to a receiving device at the address received from the send client application to notify the intended recipient of the document's transmission. This notification message is sent as a text (e.g. ASCII) message using the simple mail transport protocol (SMTP) of the Internet.

[0048] In the preferred embodiment of the invention, the receiving device is a personal computer 24. However, in alternate embodiments, the receiving device may include a printer 26, fax machine 28, network server device, Internet-compatible telephone, Internet access appliance, or personal digital assistant (not shown).

[0049] The notification message contains the uniform resource locator (URL) of the document, which allows the server to locate the document. In response to this message, the intended recipient downloads the stored document from the dedicated server 22 with a receive client application 30. The receive client application is preferably stored at the receiving device, but may be stored in a remote location that is accessible to the receiving device. The receive client application permits the recipient to receive, view, print, and/or manipulate the document.

[0050] In the preferred embodiment of the invention, the receive client application is a Web browser. Thus,

the intended recipient can copy the URL directly from the notification message, and paste it into a Web browser on the receiving computer. The Web browser then retrieves the document from the dedicated server. In alternative embodiments of the invention, the receive client application is any other software application capable of retrieving the stored document from the dedicated server while maintaining document formatting.

[0051] The send client application is readily installed on a computer from a CD-ROM, or by downloading from the Web. For example, a user who already has an account with a dedicated server provider can configure the send client application with the appropriate account information. A user who does not have such an account is directed to a URL that has the information for setting up an account.

[0052] The send client application is accessed via an application window displayed on the sending computer's desktop. The application window is displayed once the account information is properly configured. Fig. 6 is a view of an application window 32 according to the preferred embodiment of the invention.

[0053] The main function of the application window is to view the status of, and to manage send client application activity. The application window also serves as a launching pad to reach the various functions of the send client application and the configuration user interface CUI (discussed below).

[0054] In the preferred embodiment of the invention, the application window displays a main tool bar 34 for accessing main functions of the send client application. One such function is the selectable button for new package 36. Clicking on new package opens a new package window (discussed below), which allows a user to initiate a delivery of a document. Clicking on the open button 38 opens either a saved delivery parameter or a saved package window (discussed below).

[0055] In the preferred embodiment, the main tool bar 34 includes buttons that are Internet shortcuts to CUI functions. Clicking on such button launches the user's Web browser and displays the appropriate page in the CUI. In the preferred embodiment of the invention, no additional login is required in this process. Examples of such buttons include tracking 40, account 42, billing 44, and mail lists 46 buttons.

[0056] Buttons may also be provided for send client application settings. For example, a preferences dialog accessed via a setup button 48 permits the user to specify dedicated server and proxy server account information. The user can also specify whether or not to use a low-level secure communications protocol, such as Secure Socket Layer (SSL) to secure the connection between the desktop and the dedicated server for all transmissions.

[0057] The send client application can access the local address books of supported applications. In the preferred embodiment of the invention, the user selects the setup button 48 and is presented with a pull-down

menu which lists the address books supported by the invention. The user then selects the desired address book file.

[0058] A stop button 50 is used to stop transmission of all information to the dedicated server. In the preferred embodiment of the invention, once clicked, the stop button remains depressed. To resume transmission, the user clicks on the button again, and it returns to a raised position.

[0059] The menu 52 lists operational commands for the send client application. In the preferred embodiment of the invention, the file menu 54 contains commands that have the same functionalities as buttons on the main tool bar 34. Other commands provide information regarding the send client application, or are Internet shortcuts to functions of the CUI. In Fig. 6, the menu includes listings for edit 56, package 58, CUI 60, and help 62.

[0060] The application window also displays a package manager 64 that lists all document activities initiated during an application session. The package manager is an area, or set of fields in the body of the application window which lists all document activities that have been initiated during a send client application session. When the send client application is first launched, the package manager field is empty. However, as documents are sent, they are listed in the package manager.

[0061] Fig. 7 is a view of an application window 32 showing document activities 72 according to the preferred embodiment of the invention. The package manager may display the recipient(s) 66, the subject 68, and the status 70 of the delivery. The status of an active delivery may be represented as a dynamic percentage of upload completed. Other possible status labels include "completed," "error," "pending," and "on hold."

[0062] Documents may be listed, for example, in processing, or reverse processing orders. In the preferred embodiment of the invention, the document currently being processed 74 is presented in bold characters. In alternate embodiments, the current document is indicated by other means, including highlighting, flashing, or color, or is unmarked.

[0063] Clicking on a listed document 76 highlights that listing and selects the document. Multiple documents may be selected at one time. Once a document is selected, the user can use the menu 52, for example, to hold, edit, or delete the document.

[0064] A hold prevents a pending document from being processed. The document is held in a queue until it is deleted or the hold is removed. In the preferred embodiment of the invention, any or all documents in the list can be deleted. A current send is completely aborted, and an already-processed document is deleted from the window.

[0065] Editing opens a document within a new package window (discussed below). The user can then edit the document and resubmit it for sending. If a document

is edited in transmission, the transmission is aborted. The document is opened in a new package window, and the next pending document is transmitted.

[0066] Fig. 8 is a view of a package window 78 according to the preferred embodiment of the invention. The package window allows the user to specify parameters of the document delivery. A new package window is accessible from the application window, for example, by menu or tool bar selections. A package window may be saved and opened at a later time. Additionally, a package window is opened when a user sends (prints) a document from a document authoring application to the send client application.

[0067] Each document delivery transaction requires the sender to specify the recipient(s) of the delivery, the document(s) to be delivered, and the delivery options. Such delivery options include priority 80, request confirmation 82, document expiration 86, scheduled notification 88, and billing code 90. The preferred embodiment of the invention includes selectable buttons such as clear form 92, save form 94, save parameters 96, and send 98.

[0068] Any number of recipients or mail lists for a given delivery are specified in the "To:" field 110 of the package window. Each recipient must be specified by an E-mail address, alias, or mail list. The user may type an address directly into the "To:" field. Alternatively, the user may access a recipients window by clicking on the "To:" button 108.

[0069] The subject of the message is entered into the subject field 134. The message itself is entered into the message field 136. The subject 134 and message 136 fields are optional. In the preferred embodiment of the invention, the subject appears in the E-mail notification message and on an HTML cover page for the downloaded document. The message appears only in the E-mail notification.

[0070] The documents field 112 in the package window allows the user to specify any number of documents to be delivered. A document is specified in several ways. The user can click and drag the document from the sending computer desktop onto one of the application window, the package window, or onto either the icon representing the send client application, or the icon for accessing the stored document delivery parameters.

[0071] Clicking the documents button 84 in the package window allows the sender to browse local and network directories and select desired documents. If the package window is invoked from a document authoring application, the document field is automatically filled in with the current active document.

[0072] A file format field 138 allows the user to specify in what electronic format the document is saved. The send client application is readily adapted to support different formats, such as Mac Binary, Envoy, PDF, Dynadoc, and HTML. For example, a document created in a word processing application operable on one platform

can be saved in the format of another word processing application operable on a different platform.

[0073] Each delivery transaction has associated send options. In the preferred embodiment of the invention, all options have default settings which can be changed by the user prior to delivery. Settings are viewed and edited in the package window.

[0074] In the priority field 80, a user specifies the priority of a delivery, for example, as normal low, high, or urgent. Priority determines the order the document is processed by the client as well as by the dedicated server.

[0075] The request confirmation field 82 is used to prompt the recipient to confirm whether or not a document was successfully received. Request confirmation can be selected or de-selected, as desired.

[0076] The security dialog 101 allows the user to specify varying levels of advanced security measures. These levels include specifying a password 100 for basic password protection, or requesting confirmation of a password 102. Additional security provisions, such as encryption 104 or requiring the recipient to use SSL to receive 106 the document, can also be provided. If the user requires the recipient to use SSL and is not using a secure connection between the sending computer desktop and the dedicated server, the recipient is asked whether or not to secure the connection to the dedicated server.

[0077] The document expiration field 86 allows the user to specify how long a document will remain on the dedicated server for recipient availability. A default, such as ten days after notification is sent, may be provided.

[0078] The scheduled notification field 88 allows the user to specify a future date and time that the dedicated server will notify the user of a given delivery. The billing codes dialog 90 allows the user to select an optional billing code from a list associated with the user's send client application account. In the preferred embodiment of the invention, a cached list of billing codes is available. A refresh button 114 refreshes the list with the latest billing code list on the dedicated server.

[0079] Once the user has specified delivery parameters in the package window, the user initiates the document delivery by clicking the send button 98. A delivery is initiated only if both the recipient and the document fields are entered correctly. The send button is not active until both such fields are complete. If the user is working off-line, sent documents are queued for sending when the connection is eventually established.

[0080] Addresses are matched first against the current local address book. If the addresses are still not matched, they are uploaded to the dedicated server as is. The dedicated server then attempts to match addresses with a mail list. If the address is still not matched, the dedicated server appends the domain name of the account holder.

[0081] A partially completed package window may be canceled or saved using the save form button 94. The

saved package window may then be re-opened for future use.

[0082] Saved delivery parameters can be used on a recurring basis across sessions. From a package window, a user can save delivery parameters including specified send options, an address list, and/or a fixed subject or message. To save delivery parameters, a user clicks on the save parameters button 96. A dialog box prompts the user to specify a name and location for the delivery parameters to be saved.

[0083] If the saved delivery parameters contain an address list, the user can initiate a delivery by clicking and dragging a document icon onto the saved delivery parameter icon. The document provides the remaining information required for a delivery, and the send is initiated automatically. The saved delivery parameter thus serves as a dedicated mail chute to a specific set of recipients.

[0084] The existing send options may be modified or confirmed before launching the delivery. A window displaying all send parameters is opened, and the user can modify parameters or append a message before sending the document. In the preferred embodiment of the invention, the user is prompted to save any modifications to send options or existing address lists upon closing the package window.

[0085] If the saved delivery parameters do not include an address, clicking and dragging a document onto the saved delivery icon opens a package window. The saved send options and name of the document are specified in the package window. The user must specify a recipient before the document can be sent.

[0086] Saved delivery parameters are opened by clicking on the associated icon, or by selecting the appropriate main tool bar 34 or menu items. The settings are displayed in a package window and are completed or modified for a delivery. If the send client application is not open, opening the saved delivery parameters opens the application window as well as a package window. Modifications to the saved delivery parameters are preserved by replacing the existing saved parameters, or by creating a new saved delivery parameters file under a different name.

[0087] If unsaved changes have been made to the saved delivery parameters, the user is prompted to save the changes upon closing the package window. A sender can add an address list to an existing saved delivery parameter that did not previously contain an address list. The settings of the package window are saved using the "save settings as default" button 116.

[0088] Fig. 9 is a view of a recipients window according to the preferred embodiment of the invention. The recipients window 118 is used to select the recipient's name from an address book or pre-defined mail list.

[0089] In the preferred embodiment of the invention, a pull-down menu 120 allows the user to access addresses in a local address book or a mail list. For example, selecting mail list in the pull-down menu and

clicking on the refresh button 122 populates the list box 124 with the names of the mail lists stored on the dedicated server for the account for which the send client application is configured. Selecting local address book and clicking on the refresh button populates the list box with addresses from the address book specified in the preferences dialog.

[0090] Each time the recipients window is opened, the send client application displays a previously cached list of addresses. Clicking on refresh forces a refresh of the list from the appropriate source. The send client application presents the last selected source for the next send, both within and across sessions. The cancel button 135 cancels the recipients window display.

[0091] A user can select items from the list box 124 and click the "To" arrow button 126 to specify the selections as recipients. In the preferred embodiment of the invention, control-click allows selection of multiple items and shift-click selects a range of items. Recipients are presented in the recipients box 128. Recipients listed in the recipients box list are selected and removed by clicking the delete button 130 or by hitting keyboard backspace or delete keys.

[0092] When the user clicks on the "OK" button 132, items in the recipients box list are displayed in the "To:" field 110 of the package window 78 (see Fig. 8). In the preferred embodiment of the invention, mail lists have the prefix "list:" prepended to them. A user can also delete or modify recipient addresses from the "To:" field of the package window.

[0093] The specified document delivery parameters may be stored in a storage module for later modification and/or use. In the preferred embodiment of the invention, the send client application and the package window are accessed by selecting their representative icons (not shown) from the sending computer's desktop. [0094] A configuration user interface is provided for directly invoking and customizing the dedicated server. The CUI is accessed via a CUI application window displayed on a managing computer desktop. Alternatively, the CUI is accessed through any Web browser application that supports tables, or accessed through the send client application. Fig. 10 is a view of a CUI application window 140 according to the preferred embodiment of the invention.

[0095] In the preferred embodiment of the invention, the CUI is an HTML interface for invoking and customizing the dedicated server via a Web browser. This HTML interface includes modules for sending the document, tracking the document, accessing information associated with the document delivery account, managing billings for the document delivery, and managing mail distribution lists.

[0096] The CUI offers different sets of functions, depending on the user and type of account used. Individual account holders, group account managers, and group members see slightly different interfaces and are able to access and manipulate varying sets of data.

[0097] When a user initiates a CUI session, the type of account is identified by the dedicated server. The specific user is then provided with the appropriate functions and data.

[0098] In the preferred embodiment of the invention, individual account holders and group account managers have access to all delivery and account information associated with the account. Account managers therefore have access to information regarding activities of all group members using the account. Account managers are additionally authorized to create and manage member accounts. Group members have access only to information regarding the members own delivery services.

[0099] The managing computer can be the sending computer, the receiving computer, the dedicated server, or some other computer in the electronic network. The CUI includes five main functions, new package 142, tracking 144, account 146, billing 148, and mail lists 150.

[0100] In the preferred embodiment of the invention, these main functions are displayed as selectable buttons 142, 144, 146, 148, 150 on a persistent main tool bar 154. In Fig. 10, this main tool bar is displayed in a horizontal orientation, and also includes a quit button 152. However, alternative embodiments display different configurations of the application window.

[0101] A secondary tool bar 156 is provided for accessing and navigating secondary functions 164 within the main functions. In Fig. 10, the secondary tool bar is displayed in a vertical orientation. However, this configuration is for exemplary purposes only. The invention may be implemented readily to display different orientations of the main and secondary toolbars.

[0102] The secondary navigation on the secondary tool bar 156 for the CUI application window 140 includes address 166 and options 168. A help button 158 included on all secondary toolbars is used to access on-line help for the current function.

[0103] The CUI application window also includes a workspace 160 for displaying an interactive interface to an accessed function. A menu 162 lists operational commands for the CUI.

[0104] A send function mirrors that of the send client application. The send function is accessed from the new package button 142. This send function allows users to send documents from remote locations using any browser. The send function also allows documents to be sent from platforms not supported by the send client application. In the preferred embodiment of the invention, saved delivery parameters, Envoy conversion, and access to local address books are not available.

[0105] Clicking on the new package button to access the send function brings up the package window. Fig. 11 is a view of a CUI package window 170, according to the preferred embodiment of the invention. The current function is indicated by an item 192 in the secondary tool bar.

[0106] For a given delivery, a user can manually enter names into the "To:" field 172. A mail list may also be selected from a pull-down menu 174. The user may thereby view and manipulate mail lists. In the preferred embodiment of the invention, the user does not have access to a local E-mail address book.

[0107] If an item entered in the "To:" field 172 does not contain proper domain formatting (e.g. the "@" is omitted), the item is compared to the mail lists by the Server. If the item is not located in a mail list, the server appends the sender's domain name to the end of the item.

[0108] A sender inputs text into the subject 176 and message 178 fields. The sender may specify a document to be sent by typing the name of, and path to the document into the "Document:" field 180. Alternatively, the document may be specified by clicking the browse button 182 and browsing to select a document from a local or network directory.

[0109] To send multiple documents, the sender clicks on the "Add more documents..." link 184. The sender is then presented with a window (not shown) having the same format as the new package window, with the addition of four additional "Document:" fields and browse buttons. The information already entered on the previous CUI package window 170 is carried over into the new window. Thus in the preferred embodiment, a sender may specify up to five documents. In alternative embodiments, any number of documents may be specified.

[0110] The reset button 186 clears all fields in the window to their defaults. The send button 188 is used to initiate the delivery of the document with the default options. If the information input into the address form is incomplete or incorrect, the invention displays an error page (not shown) to the sender. The invention may also prompt a sender for a document's mimetype if it is not recognized. A mimetype specifies the format of a document, and is used by the recipient browser to bring up the corresponding application to display the document. In the preferred embodiment, the error page is directly edited, and the new information directly submitted. When the send is complete, a notification page (not shown) is displayed to the sender.

[0111] In the preferred embodiment of the invention, the CUI includes most of the send options of the send client application (see Fig. 8). These send options are accessed by clicking on the options button 190 to open a CUI options page. Fig. 12 is a view of a CUI options page 194 according to the preferred embodiment of the invention. Such options include priority 196, request confirmation 198, document expiration 200, and scheduled notification 202. However, because the send client application driver is not available from the server, certain send client options such as document type are not implemented. A document is therefore sent in the document's original format only.

[0112] A security function 204 is incorporated into the

preferred embodiment of the invention. The preferred embodiment of the invention supports security and encryption features permitted under current law for use in the United States. Alternative embodiments of the invention comply with any security and encryption requirements for software applications intended for export from the United States.

[0113] The CUI user may specify a password 206 that a recipient must provide to access a document. The user may also specify confirm password 208, encrypt document 210 and require SSL to receive 212. The password may be used as a secret key to encrypt the document on the server. This provides a higher level of security while the document is stored on the server. If the encrypt document function 210 is selected but the user has not specified a password, the CUI transmits an error message when the user attempts to apply the settings.

[0114] The billing code option 214 allows users to select a billing code, including "None" from a pull-down menu. The list is defined and maintained in the billing module of the CUI (see Fig. 19). The "Billing Code" text link brings users to the billing section of the CUI. Users may thereby view and manipulate billing codes.

[0115] Clicking on the reset button 216 restores the default settings. Alternatively, the current settings may be saved 218 as the default. Once the options are set, the user uses the Update button 220 to return to the package window 170. A delivery is then initiated by clicking on the send button 188.

[0116] Tracking is accessible from the tracking button 144 on the persistent main tool bar 154. The tracking search function is used to query the CUI database for information about deliveries sent from an account. A sender can therefore find out whether a recipient has received a particular document. The database archive can also be searched for records of past transactions.

[0117] Fig. 13 is a view of a CUI tracking search page 222 according to the preferred embodiment of the invention. The secondary navigation from the secondary tool bar 156 includes log 224, search 225, report 226, preferences 228, and help 158. The current function 192, search 225, is identified. The tracking button on the main tool bar displays a record of all deliveries sent from the account as a delivery log (not shown).

[0118] Account managers are permitted to track all deliveries initiated from a group account. Group members are permitted to track only those deliveries initiated personally by the member.

[0119] The format of the delivery log is specified in tracking preferences (see Fig. 14). The format chosen applies to both the delivery log and the tracking report (see Figs. 15-17). The preferred embodiment of the invention includes navigation buttons to permit the user to access previous, or subsequent log pages. Information regarding an individual delivery may be displayed on the delivery log, along with an indication of the total number of deliveries logged.

[0120] The subject of each listing in the log links to a package detail report (not shown) about the specific delivery. A detail report contains send parameters of each delivery, including a link to the document if not expired, the mimetype, and the message. The detail report also contains the status of the delivery to each recipient, and the charges applied to the transaction. Users can click on log 224 on the secondary tool bar 156 to return to the top level log.

[0121] The search function allows users to pinpoint information about, and the status of, a specific delivery or set of deliveries. The user specifies any combination of search criteria to identify the deliveries of interest. If multiple criteria are specified, the search engine performs a logical "AND" search among all the criteria.

[0122] In the preferred embodiment of the invention, the search page graphical user interface (GUI) is simplified. A short list 230 of common searchable fields is presented on the Search page. The short list contains five search criteria:

[0123] The "To:" field 232 allows a user to search by the intended recipient's full or partial E-mail address of the recipient. Partial e-mail addresses allow the user to search by domain name.

[0124] The "From:" field 234 allows an account manager to search according to the originator of the delivery. The account manager selects a member's e-mail address from a pull down menu. For group members and individual account holders, this given user's e-mail is provided and cannot be changed.

[0125] The "Subject:" field 236 allows a user to enter keywords which may be found in the subject field of a document.

[0126] The "Document:" field 238 allows a user to perform a text search on the name of the document. A user can type in the name of the document, or browse through the list of documents to select a document.

[0127] The "Send date:" field 240 allows a user to search for deliveries sent on, before, or after a specific date.

[0128] Clicking on the search button 242 initiates the query and returns a report with all deliveries matching the query. Clicking on the reset button 246 clears the form to its default setting.

[0129] Clicking on a "More Options..." button 248 at the bottom of the short form brings the user to a page having a second, expanded list (not shown) of searchable fields, including all fields from the short list. In the preferred embodiment, the additional fields in the expanded list include:

[0130] The billing code: field allows a user to select from a pre-defined list in a pull down menu.

[0131] The "Delivery status:" field allows a user to select from a menu of delivery statuses. Delivery status options include: any, received, not received (includes both failed notification and not picked up), confirmed, not confirmed, pending notification and failed notification. The user may also search document expiration,

scheduled notification date, receive date, and message fields.

[0132] The search results are presented in a tracking report. The tracking report is presented as a table in a format specified in the tracking preferences dialog. Fig. 14 is a view of a CUI-tracking report preferences dialog 250 according to the preferred embodiment of the invention.

[0133] The Dialog permits the user to select a document format 252, or to define a new format 254. In the preferred embodiment of the invention, a user can select from two pre-formatted reports, basic format and billing code format. Both summary and detail information reports are available in each format.

[0134] The dialog allows the user to specify the number of rows per page 256. Additionally, the user selects whether to show recipient summary information 258, or detail information 260.

[0135] Clicking on update 262 saves all changes and returns the user to the report or page from which the user accessed the tracking report. If the user returns to a report, it is displayed with the new preferences settings. The dialog is reset using the reset button 264.

[0136] Fig. 15 is a view of a recipient summary tracking report in basic format 266 according to the preferred embodiment of the invention. When search results are displayed, the secondary navigation in the secondary tool bar 156 indicates that the sender is in report mode 226. The elements and behavior of the tracking report are consistent with those of the delivery log.

[0137] In the preferred embodiment of the invention, the deliveries are sorted by date and presented in reverse chronological order. However, in alternative embodiments, the deliveries are presented in chronological order, or are sorted, for example, by recipient. The next page of delivery listings is accessed by clicking on the next button 284.

[0138] A recipient summary tracking report lists, in the "Recipient(s):" field 270, only the name of the first recipient 268 of a particular delivery, or the first recipient on the mail list to which that delivery was sent. An indication (...) is placed next to the name if there are more names on the list. The number of recipients of the delivery is listed in the "Received:" field 272 and the number notified is listed in the "Notified:" field 274. This information is totaled 276 across all recipients.

[0139] For example, the most recent delivery shown in Fig. 15 is the party invite listed in the "Subject:" field 278. The date the party invite was sent was January 22, 1997, as is indicated in the "Sent:" field 280. The tracking report shows that a total of three party invite documents were sent. All three recipients were notified, and received the document. Only the first recipient 268, "jane@isp.com," is listed in the "Recipient(s):" field 270.

[0140] Fig. 16 is a view of a recipient detail tracking report in basic format according to the preferred embodiment of the invention. A recipient detail tracking report 282 lists in the "Recipient(s):" field 270 each recipient of

each delivery. The "Received:" 272 and "Notified:" 274 fields list the specific dates that each recipient was notified of, and received the delivery. For example, Fig. 16 separately lists the three recipients of the party invite, and their notification and receipt dates.

[0141] The recipient detail tracking report also expands every mail list. In the preferred embodiment of the invention, mail lists are only expanded for deliveries that have been processed. Future scheduled deliveries and deliveries in progress are indicated as such.

[0142] Fig. 17 is a view of a recipient detail tracking report in billing code format 286 according to the preferred embodiment of the invention. The billing code format displays the billing code 288 and sorts results by billing code and date.

[0143] The CUI account management functions are available from the main tool bar button labeled "Account" 146. Account functions vary according to the type of account and the type of user, such as group account manager, individual account holder, and member account holder. The server software identifies a user's account type and makes the appropriate functions and information available.

[0144] All users are able to view administrative account information on record for the respective user's account, including account balance, and can also change their password. Group account managers, however, have extended capabilities. They can edit group members' account information as well as create new accounts. Thus, the secondary navigation of the secondary toolbars displayed to group account managers includes functions such as Information: 302, view members: 304, and add member: 306 (see Fig. 18).

[0145] The Information page (not shown) displays basic information about the group account that is stored on the dedicated server. Such basic account information includes:

- the name of the account
- type of account
- date it was created
- date it was last accessed
- the number of current members out of the maximum allowed.

[0146] Account managers can view and manage the current member list via the Members page (not shown).

[0147] Account holder information includes:

- name of the manager
- e-mail address
- company name
- address

[0148] The basic account information and the account manager information cannot be edited.

[0149] The group account password can be changed from the Information page. The manager enters the

existing password and the desired new password, and must confirm the new password. The manager submits the new password by clicking on Update.

[0150] In the preferred embodiment, the information page also includes a field which informs the manager when the password was last changed. If the password has never been changed, this field presents the creation date of the account. A link may also be provided to a server manager who is authorized to make changes to accounts.

[0151] Managers can view a list of members by clicking on the members text link on the Information page, or by selecting the view members function of the secondary tool bar 156. Fig. 18 is a view of a group account manager account - view members window 288, according to the preferred embodiment of the invention. In one embodiment, managers use a link (not shown) to Preferences (not shown) where the managers can specify the format, the number of rows per page, and the sorting order of the View Members table.

[0152] The view members page displays the name 290 of the group account, and the number 292 of the members displayed out of the total number. The list of members includes the account manager, and is presented in a table which lists the member account names 294, the member names 296, the date created 298, and the date last accessed 300. Clicking on a member's name brings up a "Mailto:" box (not shown), pre-addressed to the member.

[0153] Clicking on the account name allows managers to view and edit individual member account information. This information is displayed on a member account information page (not shown) which is similar in format to the group account information page. Basic member account information includes the following (editable information is noted):

- group account
- member account (editable)
- date created
- date last accessed

Member information

[0154]

- member name (editable)
- e-mail address (editable)

[0155] Managers cannot view the member's password, but can change the password on the member account information page by specifying a new password and confirming it. The date of the last password change (not shown) by either manager or member is also displayed. Any changes made to the information on this page can be submitted by clicking on update (not shown). Reset (not shown) restores the previously stored information.

[0156] Member accounts can be completely deleted by clicking on a delete button on the member account information page. Prior to deleting the account, the dedicated server posts a confirmation page notifying the manager of the impending action and requesting confirmation before proceeding. When the member account is updated or deleted, an updated view members window is displayed.

[0157] Managers can add members by clicking on the add member link in the secondary tool bar 156. A form (not shown) is displayed prompting the account manager for the information required to create a member account. The form indicates the group account to which the member is added, and the number of the member out of the maximum total members allowed. The information required includes:

- member account name (created by the manger)
- member's name
- member's e-mail address
- password (and confirm password)

[0158] Clicking on add (not shown) creates a new account and returns the manager to an updated view members window. Clicking on reset (not shown) clears the form.

[0159] Because individual accounts have no group members aside from the account holder, such individual account holders do not have member information or functions. The secondary tool bar 156 includes only information (not shown) and help (not shown.) The information displayed from the account information page is the same as that available from the group account information page, except for the number of current members.

[0160] Member account holders also do not have member management functions, and the secondary tool bar includes only information (not shown) and help (not shown). Member account information contains the same basic information as that viewed by managers. However, members are only able to edit e-mail address information.

[0161] In the preferred embodiment, members can change their own passwords on the member account information page. They must enter the current password, the new password, and then must confirm the new password. However, in alternative embodiments, members may only be able to change their passwords via the account manager.

[0162] The billing button 148 on the main tool bar 154 gives access to billing code mode management and invoice functions. Clicking on the billing button displays a table 320 of defined billing codes. Fig. 19 is a view of a billing codes window 308, according to the preferred embodiment of the invention.

[0163] Secondary navigation for billing on the secondary tool bar 156 includes billing codes 310, add codes 312, create invoice 314, view Invoice 316, preferences

318, and help 158.

[0164] The table indicates the total number of codes and which ones are currently being viewed 322. In the preferred embodiment of the invention, billing codes are up to 25 characters long and are composed of letters, numbers or characters.

[0165] Each billing code 324 has an optional plain English description 326 or name associated with it. In billing preferences (see Fig. 24) the user specifies whether to sort the billing codes by code or by description, and how many rows to display per page. Preference settings 328 are displayed with the table. Next 330 and Previous (not shown) buttons allow the user to view additional pages of billing codes.

[0166] Two levels of billing codes are provided for group accounts. The group manager maintains a list of codes that are accessible by all group members. Group members can select their own subset of codes from the group list for easy access to frequently used codes.

[0167] Members cannot edit or create billing codes. They must select codes from the list created by the manager to add to their personal list. Members can specify whether to list group or personal billing codes in billing preferences.

[0168] Clicking on a hot-linked billing code allows users to edit or delete the code or its description. Fig. 20 is a view of an edit billing codes window 332, according to the preferred embodiment of the invention. Users can edit a billing code or description from the appropriate fields 338, 340 in the dialog. The information in the fields is cleared using the reset button 342.

[0169] Changes are saved by clicking update 334, which returns the user to the billing code table displaying the updated information. Users may also delete 336 codes and descriptions from this dialog. Because group members cannot edit group billing codes, group billing codes are not hot-linked when viewed by a group member.

[0170] The add codes function 312 in the secondary navigation is used to add items to a personal billing code list. Fig. 21 is a view of an add billing codes dialog 344 according to the preferred embodiment of the invention.

[0171] Managers and individual account holders enter a new code into the "Enter Billing Code:" field 346. Any associated optional description is entered into the "Description:" field 348 in the form provided. The add button 350 is clicked to add the new information to the billing code list. The replace button 352 is clicked to replace information in the billing code list.

[0172] Billing codes can also be uploaded 354 from a text file. A browse button 356 is used to locate the appropriate text file for uploading. This text file either replaces or is added to the existing billing code list. When new codes are successfully added, the user is presented with an updated billing code list.

[0173] Group members can only add codes from the group billing code list to their personal code list. When

group members click on add codes, they are presented with a list box of codes from the group list. They may then select multiple codes from the list box. Once the desired codes are selected, the member clicks on the Add button to add the selected codes to their personal list.

[0174] Clicking on the create invoice 314 link allows the user to create an invoice. Fig. 22 is a view of a create invoice window 358, according to the preferred embodiment of the invention. The dialog is a search screen which allows the user to specify which deliveries to bill for the current invoice. Deliveries are billed by billing code or by recipient.

[0175] The user selects a billing code or set of billing codes from a list 360 or enters the e-mail address 362 of the recipient. The list contains the billing codes and associated descriptions indicated in billing preferences. Current preferences are displayed 364.

[0176] The user also specifies a date range for the invoice's billing period 366. Once the appropriate information is entered, the user clicks create 368 to initiate the query and generate the invoice. Reset 370 clears all entries.

[0177] The query result is presented in a pre-formatted basic invoice report window 372 in view Invoice mode, as shown in Fig. 23. The billing code 374 and billing period 376 are displayed, along with the table 378 containing the query results.

[0178] The table displays the subject 384 of each delivery, the date sent 390, and the recipient(s) 392. The price 380 and the total 382 of the deliveries are also indicated.

[0179] Invoice format is specified in the billing preferences. The subject 384 of each delivery is hot-linked to the package detail report, described above. If the package detail is accessed, the navigation state remains in billing/view invoice. Clicking on view invoice 316 returns the display to the invoice report.

[0180] The export button 386 allows users to export the report data as a tab-delimited text file for integration into other existing billing systems. Invoice report preferences 388 (excluding the mark-up rate) are also displayed.

[0181] Billing preferences 318 allow users to specify the preferences which affect billing code management and invoice report formats. Fig. 24 is a view of a billing preferences dialog 394 according to the preferred embodiment of the invention.

[0182] A pull-down 396 allows group members to choose to use a personal billing code list or a group billing code list maintained by the account manager. All users choose to display lists by billing code 398, or by description 400. This selection affects the display in selection boxes in send options and invoicing.

[0183] The selection also affects the presentation of the billing codes display table. If display is by billing code, then the first column is billing code, and the list is sorted by billing code. If display is by description, the

first column is description and the list is sorted by description. The user specifies the number of rows displayed 402 per page.

[0184] The user also specifies the rate 404 to charge clients. This rate can be a flat charge 408, or may include a percentage mark-up 406 on top of the costs charged by the user's Internet services provider. The information displayed in the billing preferences dialog can be updated 405 or refreshed 407.

[0185] For the invoice report, the user may select a predefined format 410, or define 412 a new format. In the preferred embodiment, the user selects from three predefined formats the basic invoice, spec invoice, and billing code invoice formats. The basic invoice format has previously been shown in Fig. 23.

[0186] Fig. 25 is a view of an Invoice report in spec invoice format according to the preferred embodiment of the invention. The spec invoice 414 displays the total number 416 of recipients for each delivery as well as the size 418 of the document. This information is sorted chronologically.

[0187] Fig. 26 is a view of an invoice report in billing code invoice format according to the preferred embodiment of the invention. The billing code invoice format 420 is sorted by billing code 422, as well as by date.

[0188] The CUI allows publishers and other users to create and manage distribution lists. Fig. 27 is a view of a mail list page 424 according to the preferred embodiment of the invention. Mail list functions are accessible from the main tool bar 154. Secondary navigation includes mail list 426, create list 428, preferences 530 and help 158.

[0189] There are two levels of mail lists for group accounts, i.e. group and personal. Group lists are managed by the account manager and are accessible to all group members. A group member can define a personal list accessible only by that group member. Each member can specify which set of lists to use in their mail list preferences.

[0190] Clicking on the mail list button 150 on the main tool bar 154 displays a table 432 listing existing mail lists 434. The table also presents the total number 436 of recipients on each mail list and the date 438 the mail list was most recently modified. The preferences settings 440 are also displayed.

[0191] In mail list preferences (not shown), the user specifies whether to sort the items by the name of the mail list or by date. Current preferences are displayed in the mail lists dialog. Next and previous buttons (not shown) may be provided to navigate between pages of mail lists.

[0192] Clicking on the hot-linked name 442 of a mail list brings up a mail list detail for the selected mail list. Fig. 28 is a view of a mail list detail window 444, according to the preferred embodiment of the invention.

[0193] The mail list detail page displays general information about an existing mail list and allows the user to view and manage mail list addresses. Group members

cannot manipulate group mail lists. Therefore, the mail list detail of group lists does not display fields for editing. Group members can, however, edit personal mail lists.

[0194] Account Managers can manipulate group mail lists. The detail 444 presented to account managers displays the name 446 of the mail list in an editable form. To rename the list, the user changes the name in the form and clicks on the update button 448. Users may also delete 450 the entire mail list or add addresses 452 by clicking on the appropriate button. The total recipients 454 and date last modified 456 are also displayed.

[0195] The detail also displays the mail list addresses 458. In the preferred embodiment of the invention, the first page of the complete address list is displayed in accordance with the number of rows per page specified in the mail list preferences. The detail indicates which addresses out of the total are displayed. Next and previous links (not shown) may be provided to navigate between multiple pages of addresses.

[0196] The user can also view a select set of addresses by specifying a query in the field 460 provided. For example, an e-mail address or a portion of an address such as a domain name can be specified. Clicking on the view button 462 then displays a table 464 of matching addresses 458. The table indicates which addresses 466 out of the total matching set of addresses are displayed.

[0197] The user edits or deletes individual addresses in the table by clicking on the appropriate address. An edit page (not shown) with update and delete buttons is then displayed. When the address is updated or deleted, users are returned to an updated mail list detail page.

[0198] From the detail page, users can also delete multiple addresses at a time. Clicking on the "delete items on page" button 468 deletes all the addresses in the table. Clicking on "delete all matching items" 470 deletes all items which matched the query, whether or not the addresses are visible on the current page. A warning message asking the user to confirm the action is displayed before the dedicated server actually deletes the addresses. Once the addresses are deleted, the detail page is immediately updated and presented to the user.

[0199] Clicking on the add addresses button 452 in the mail list detail 444 displays the add addresses page. Fig. 29 is a view of an Add Addresses window 472 according to the preferred embodiment of the invention. The name of the current mail list 474 is displayed at the top. The name is also linked to the mail list detail page.

[0200] The user can add additional addresses by manual entry 476, by uploading them from a file. The user can enter a file name 478, or use the browse button 480 to search all files. Names may also be obtained from an existing mail list 482 and merged with the current mail list. The additional addresses are added 484 to the current address list or replace 486 the current list. After the names are submitted, the users are returned

to an updated member detail page with a line at the top confirming the addition or replacement that just occurred.

[0201] The user can create a new mail list by clicking on the create list link 428 from the secondary navigation. In the preferred embodiment of the invention, the create mail list page (not shown) is similar to the add addresses page. However, in the create mail list page, the user is prompted for the name of the mail list.

[0202] The user can manually enter addresses in the provided text box. Alternatively, the user can upload addresses from a file or copy addresses from an existing mail list. However, because the user is creating a new list, there is no option provided to replace an existing list. Clicking add creates a mail list with the specified names and addresses. The user is presented with an updated mail list report, with the new list information included.

[0203] The invention also provides security for restricting access to the system to an authorized user. The types of security supported by the invention include authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication. This security is provided by a security framework that includes at least one security module, in at least one of the send client application, the receive client application, and the CUI.

[0204] Fig. 30 is a flow chart of the method for delivering a document over an electronic network, according to the invention. The sending computer establishes a session (500), for example, over the Internet. The sending computer then delivers the document to a dedicated server (505) over this electronic network, using a send client application.

[0205] The send client application preferably includes modules for sending documents, listing document activities, tracking documents, specifying and storing document parameters and for providing security features (510). Any or all of these modules may be accessed during a particular session.

[0206] The dedicated server stores the document (515) and forwards an electronic notification message to the receiving device (530). The dedicated server is managed via a configuration user interface (520). The configuration user interface preferably includes modules for sending documents, tracking documents, accounting, billing, generating mail lists, as well as a security feature module (525).

[0207] In response to the notification message, the receiving device downloads the document (535) from the dedicated server using a receive client application. The receive client application preferably includes modules for downloading, viewing, and manipulating the document, as well as for providing security (540).

[0208] Although the invention is described herein with reference to the preferred embodiment one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing

from the spirit and scope of the present invention. The invention is readily constructed and configured by one skilled in the art, using well-known programming techniques and equipment.

5 [0209] For example, the placement and contents of the toolbars and menus in the desktop displays described herein is for exemplary purposes only. Furthermore, the functions of the invention may be accessed by alternate means, including icons, and keyboard text entries.

10 [0210] In one embodiment of the invention, the notification message regarding a document delivery is received by a notification receiving device. The document can then be retrieved by a receiving device that is either included in the notification receiving device, or is separate therefrom. For example, the notification message can be received on a pager or personal digital assistant, and the document received on a personal computer using a Web browser.

15 [0211] The sender driven certificate enrollment system (SDCE) 42 enables corporations, publishers and individuals to securely distribute documents electronically, by allowing the sender to initiate and control the implementation of digital certificate enrollment to one or more recipient clients.

20 [0212] Fig. 31 shows a basic certificate enrollment system 1342a implemented between a sending computer 1352 and a receiving computer 1370 across a network 1344, which may include an internet. Fig. 32 shows a certificate enrollment system 1342b implemented between a sending computer 1352, a SDCE server 1358 and a receiving computer 1370. Fig. 33 shows a certificate enrollment system 1342c implemented between a sending computer 1352, a SDCE server 1358, a database server 1362 and a receiving computer 1370. Fig. 34 shows a certificate enrollment system 1342d implemented between a sending computer 1352, a SDCE server 1358, a database server 1362, a certificate server 1388 and a receiving computer 1370.

30 [0213] The sender driven certificate enrollment system 1342 enables the sender 1352 of a document 1312 to initiate the generation of a digital certificate 1345, (see Fig. 35) on behalf of an intended recipient 1370 of a document. A document 1312 can mean a specific computer file or more generally any discrete collection of data. The sender driven certificate enrollment system 1342 simplifies the associated complexity of generating a digital certificate for an intended recipient 1370 of a document, and transfers the primary burden of certificate generation from the recipient 1370 (which many systems support today) to the sender 1352. Fig. 35 shows a digital certificate 1345, which denotes a key pair comprising a public 1332 and private key 1340, where the public key 1332 is associated with a specific entity, such as an intended recipient 1370, and is published.

35 [0214] One of the main problems associated with

secure document delivery stems from the challenge of encrypting a document 1312 with the public key 1332 of the intended recipient 1370. In particular, the intended recipient 1370 of a document may not have a digital certificate 1345. In the absence of a digital certificate 1345 of the recipient 1370 which is accessible by the sender 1352, the sender 1352 of a document 1312 cannot encrypt the document 1312 with the recipient's public key 1332, and hence cannot be assured that the document 1312 can be protected from unsolicited access. The sender driven certificate enrollment system 1342 allows the sender 1352 of a document 1312 to initiate the process of dynamically generating a digital certificate 1345 for the intended recipient 1370, thereby imposing minimum requirements for the intended recipient 1370.

[0215] The sender driven certificate enrollment system 1342 transfers the burden of certificate generation from the recipient 1370 of a given document 1312 to the sender 1352. The sender driven certificate enrollment system 1342 exploits the fact that, in the context of document delivery, often the sender 1352 of a document 1312 has unique and specific information regarding the intended recipient 1370. Suppose, for example, an attorney sends a document to a client 1370. The attorney 1352 likely has a record associated with the client 1370 which contains specific information, such as the client's e-mail address, physical address, telephone number. The client record may also contain confidential information, such as the client's social security number, drivers license number, or even credit information.

[0216] Typically, it is this type of confidential information which is utilized to authenticate a given individual or entity 1370, and hence generate a digital certificate 1345. Highly confidential and specific information yields a high level of authentication, and hence a secure digital certificate.

[0217] Therefore, the sender driven enrollment system 1342 exploits the fact that the sender 1352 often knows significant and confidential information regarding an intended recipient 1370 of a document 1312. The use of this confidential information by the sender 1352 to generate a digital certificate 1345 minimizes the burden imposed on the recipient 1370 to confirm their identity. The digital certificate 1345 is then utilized by the sender 1352 to securely send the document 1312 to the intended recipient 1370.

[0218] System Implementation. In the example above, a sender attorney 1352 wishes to send a confidential document to an intended recipient client 1370. For a client 1370 that does not currently have a digital certificate 1345 accessible to the attorney 1352, the attorney 1352 can invoke the sender driven enrollment system 1342 to generate a digital certificate 1345 for the client 1370.

[0219] First, the sender driven enrollment system 1342 checks or queries a database 1346 to determine if a digital certificate 1345 exists for the recipient client 1370. If not, the sender driven enrollment system 1342

conducts a database query to pull up a record for the client 1370, which typically includes client specific and confidential information.

[0220] The sender driven certificate enrollment system 1342 then generates a certificate digest 1347, as shown in Fig. 36. This certificate digest 1347 contains most of the information necessary to generate a digital certificate 1345 for the client 1370, including the client specific data 1348, and the type of certificate to generate 1349 (e.g. an X.509 certificate). In a preferred embodiment, the certificate digest 1347 is forwarded to a secure SDCE server 1358. The SDCE server 1358 then "contacts" the client 1370 seeking independent confirmation of the confidential information 1348. For example, in a preferred embodiment of the invention, the SDCE server 1358 forwards an e-mail message to the client 1370 with a unique, dynamically generated URL (uniform resource locator). The client 1370 can then "click" or access this URL through a standard web browser. Accessing the URL begins a direct interaction, or SDCE conversation 1368, between the client 1370 and the SDCE server 1358.

[0221] The client 1370 is typically asked to input one or more pieces of confidential information 1348 to the SDCE server 1358. In a preferred embodiment, the conversation takes place over a secure socket layer (SSL) channel between client 1370 and the SDCE server 1358, and utilizes HTML forms.

[0222] The SDCE server 1358 then attest whether the client 1370 is correct, by comparing input information to the stored client information 1348 within the stored certificate digest 1347. On a match, the SDCE server 1358 forwards the certificate digest 1347 over a secure channel to the recipient client's desktop 1372, and also distributes software to the recipient client 1370, which uses the certificate digest 1347 to generate a key pair 1332, 1340 on the recipient system. In the preferred embodiment of the invention, this software is simply a Java applet, transparently forwarded to the recipient 1370 through the browser. The generated private key 1332 is stored on the recipient system 1370, preferably using the PKCS12 format. The public key 1332 is forwarded back to the SDCE server 1358, which typically registers both the public and client information as the digital certificate 1345 on a certificate server 1388, such as an LDAP or an Entrust certificate management server (of Entrust, Inc., Ottawa, Canada).

[0223] The sender (e.g. the attorney) 1352, can now access the stored public key 1332 for the intended recipient client 1370, encrypt the document 1312 intended for the recipient client 1370 with the public key 1332, and then send the encrypted document 1336 to the client 1370. The client 1370, in turn, decrypts 1338 the encrypted document 1336 with [the public key and] the corresponding private key 1340, which is now resident on the private recipient system 1370.

[0224] Fig. 37 shows the first stage 1350 of the sender driven certificate enrollment system 1342. A sender

1352 initiates the generation of a certificate for a recipient 1370 at step 1356, by contacting an SDCE server 1358 and forwarding basic information to identify the recipient 1370, such as an e-mail address.

[0225] The SDCE server 1358 then queries a database 1346, at step 1360, for confidential information 1348 specific to an intended recipient 1370, such as a social security or personal address. The database 1346 may reside at any of a number of locations, such as within a separate database server 1362, or within the SDCE server 1358.

[0226] If usable confidential information 1348 exists for an intended recipient 1370, it is transferred, at step 1364, as a data record to the SDCE server 1358. The SDCE server 1358 then uses the data record to generate a certificate digest 1347, at step 1365, which is later used to attest the recipient 1370 and to generate a digital certificate 1345.

[0227] Fig. 38 shows the second stage 1366 of the sender driven certificate enrollment system 1342, referred to as an attestation conversation. The SDCE server 1358 takes the certificate digest 1347 and initiates a direct interaction, at step 1368, with the intended recipient 1370 of a document 1312. This direct interaction 1368 solicits client specific data 1348 from the intended recipient 1370.

[0228] In a preferred embodiment of the invention, the SDCE server 1358 sends an e-mail message with a dynamically generated Uniform Resource Locator (URL). The recipient 1370, by clicking on the generated URL, invokes a direct interaction 1368 with the SDCE server 1358. At this point, the SDCE server 1358 presents HTML forms soliciting specific information from the recipient 1370.

[0229] The HTML forms and requested private information 1348 may vary, depending on the level of security desired for the document 1312 to be sent to the recipient 1370. For example, for a document that does not require a high level of security, the forms might simply request a confirm button. For a document that requires a higher level of security, the form might ask the intended recipient 1370 to submit specific private information 1348, such as a personal address, a social security number, and employee number or personal identification number (PIN). In a preferred embodiment of the invention, this interaction between the SDCE server 1358 and the recipient 1370 takes place over a secure channel using SSL.

[0230] Using the forwarded private information 1348, through step 1374, the SDCE server then attests the recipient 1370 by comparing the forwarded data 1348 to the certificate digest 1347 for the intended recipient 1370. If the forwarded information 1374 and the appropriate stored information 1348 in the certificate digest 1347 match, the recipient 1370 is authenticated, at step 1375, and the process continues to the next stage. If the forwarded 1374 information and the appropriate stored information 1348 in the certificate digest 1347 do not

match, the sender 1352 is notified that no digital certificate 1345 has been generated (Fig. 41).

[0231] Fig. 39 shows the third stage 1376 of the sender driven certificate enrollment system 1342, referred to as public/private key pair generation. Assuming that the private information 1374 solicited over the attestation conversation stage 1366 matches the certificate digest 1347 at the SDCE Server 1358, the SDCE server 1358 then forwards software and the certificate digest 1347 to the recipient system 1370, at step 1378. The forwarded software utilizes the certificate digest 1347, and information local to the recipient computer 1370, to generate a digital certificate 1345, comprising private/public key pair 1332, 1340. The key pair 1332, 1340 is sent to and stored locally on the sender system 1352. In a preferred embodiment, the public/private key pair 1332, 1340 is stored in a PKCS12 format. The public key 1332 and a reference to the certificate digest 1347 for the recipient 1370 is then forwarded from the receiver 1370 to the SDCE server 1358.

[0232] Fig. 40 shows the fourth stage 1384 of the sender driven certificate enrollment system 1342, referred to as forwarding and registration of the receiver public key 1332. At this stage in the process, the public key 1332 for the intended recipient 1370 has been forwarded from the recipient system 1370 to the SDCE server 1358. The SDCE server 1358 forwards the public key 1332 and the certificate digest 1347, combined as a digital certificate 1345, to a certificate server 1388, at step 1386. In a preferred embodiment, the certificate server 1388 is an LDAP (Lightweight Directory Access Protocol) server. The SDCE server 1358 then sends a notification back to the sender 1352, at step 1390, that indicates that the document 1312 can now be encrypted 1334 with the public key 1332 of the recipient 1370, as shown in Fig. 3. The encrypted document 1336 is then delivered to the recipient 1370, typically across a network or internet architecture 1344. The recipient 1370 then uses their own private key 1340 to decrypt the information, as shown in Fig. 4.

[0233] Implementation. This section provides an overview of the components to construct a sender driven certificate enrollment system 1342. Some of the components, such as the certificate server 1388 do not require any customization or development. Fig. 41 is a basic flow chart that describes the flow of control for the system.

[0234] Sender Desktop Client Software. On the desktop 1354 of the sender computer 1352, the sender driven certificate enrollment system 1342 includes software which communicates with the SDCE server 1358 and the certificate server 1388 to query the public key 1332 associated with the recipient 1370. The recipient software component, upon retrieval of the public key 1332 for the recipient 1370, typically encrypts a document 1312 with the public key 1332 and then forwards the document to the SDCE server 1358 for subsequent delivery to the recipient 1370.

[0235] SDCE Server Software. The SDCE Server software, in a preferred embodiment of the invention, includes a HTTP Web Server with a customized filter to intercept and redirect all HTTP requests, a e-mail server to forward notifications on to an intended recipient 1370, and the basic software and logic to query a database server, to generate a certificate digest 1347 (as described above), and to interact with all other components of the system.

[0236] The Web server is a primary interface between the SDCE server 1358 and the intended recipient 1370 of a document 1312, in which the SDCE server 1358 assists in the construction of a digital certificate 1345.

[0237] In a preferred embodiment of the invention, the SDCE server software initiates an attestation conversation 1366 (Fig. 38) with the intended recipient 1370, by dynamically generating a private URL. The private URL contains a key to uniquely identify the recipient 1370, and then forwards this "key" to the recipient over a standard e-mail notification. When the recipient 1370 accesses this "key" (which in fact is a private URL), the SDCE server 1358 associates the key with a given certificate digest 1347, and then through the Web interface, conducts the attestation conversation 1366, to verify that the given recipient 1370 matches the parameters of the certificate digest 1347.

[0238] Recipient Client Software. The sender driven certificate enrollment system 1342 creates a public/private key pair from a certificate digest 1347, which is forwarded from the SDCE server 1358 to the recipient system 1370. Client software on the recipient computer takes the certificate digest 1347, constructs the public/private key pair 1332, 1340 on the recipient desktop 1372, stores these keys 1332, 1340 on the recipient system 1370, and then forwards the public key 1332 to the SDCE server 1358.

[0239] In a preferred embodiment, the recipient client software is a Java applet, which is transparently and dynamically downloaded via a web browser, in which the recipient simply accesses an URL, as described above.

[0240] Certificate Server. The invention makes use of basic digital certificate management. The certificate server 1388 includes query ability, which determines if a digital certificate exists for a recipient given a specific user profile (e.g. an e-mail address and identifier). The certificate server 1388 also includes update ability, which allows a programmatic interface to add a new certificate to the server's database. In preferred embodiments, LDAP, X.500, or proprietary certificate servers such as a Entrust server can be used as certificate servers 1388.

[0241] Database Server. In a preferred embodiment of the invention, the SDCE server 1358 queries a database 1346 containing recipient information to construct a certificate digest 1347. In a basic embodiment, the sender's desktop 1354 can query an internal database 1346, or the sender's desktop 1354 can simply load

information directly from the desktop 1354. The preferred database query provided by a SDCE server 1358 supports more scalability and extensibility.

[0242] In addition to the basic design for the invention, there remains situations wherein no recipient data 1348 exists which is readily accessible from the senders system 1352, either directly from the desktop 1354 or via a database query. In this case, the sender driven enrollment system 1342 still retains value. While the certificate digest 1347 contains limited information 1348, the level of attestation is also limited. However, basic attestation can still take place, and the system 1342 still simplifies the process of generating a basic digital certificate 1345 for the recipient 1370. In this case, the system behaves exactly as designed, with the exception being a more simplistic conversation 1366 and certificate digest 1347.

[0243] Fig. 41 is flow chart 1302 that describes the basic decision tree behind the sender driven certificate enrollment system 1342.

[0244] At step 102, the sender 1352 queries the certificate server 1388 for the public key 1332 of an intended recipient 1370 for a document 1312. If the public key 1332 exists, the document 1312 is encrypted with the public key 1332, and is sent to the recipient 1370, at step 104. If the public key 1332 doesn't exist, the sender queries the SDCE Server 1358 for a certificate digest 1347 for the intended recipient 1370, at step 1356.

[0245] The SDCE server 1358 then queries the database 1346 for information 1348 regarding the intended recipient 1370, at step 1360. If the information exists and is already stored in the database 1346, the SDCE server 1358 generates a rich certificate digest for the client 1370, at step 1365. If no information 1348 exists and is stored in the database 1346, the SDCE server 1358 generates a simplified certificate digest 1347, at step 1364.

[0246] At step 1368, the SDCE server 1358 initiates an attestation conversation 1366 with the recipient 1370. If there is no match to the information 1348, the SDCE server 1358 notifies the sender 1352, at step 106, and there is no generation of a key pair 1332, 1340. If there is a match, a private/public key pair 1332, 1340 for the recipient 1370 is generated on the recipient system 1370, at step 1380. The key pair is then forwarded to the SDCE server 1358, at step 1382. At step 1388, the SDCE server registers the certificate for the intended recipient 1370 with a certificate server 1388. At step 1390, the SDCE server notifies the sender 1352 of the digital certificate 1345. The sender 1352 can then encrypt the document 1312 with the generated public key 1332 of the intended recipient 1370, as shown in Fig. 3. When the encrypted document 1336 is sent to the recipient 1370, typically over a network 1344, the recipient 1370 can decrypt the encrypted document 1336, using the stored private key 1340, as shown in Fig. 4.

[0247] Although the sender driven certificate enroll-

ment system and its methods of use are described herein in connection with use in the Internet, the invention may be applied to any of a wide variety of networks, including internets, intranets, LANs and WANs, or any combination thereof, as desired. As well, the invention may be applied to a wide variety of computer platforms, servers, communication protocols, cryptography protocols, or any combination thereof, as desired.

[0248] Although the present invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow. Accordingly, the invention should only be limited by the Claims included below.

Claims

1. An apparatus for managing and delivering documents comprising:
 - a send client application (20) for delivering at least one document (16) as a single package from a sending computer (14) over an electronic network (18) during a session;
 - a dedicated server (22) for storing said at least one document (16) from the sending computer (14) and for forwarding an electronic message to a receiving device (24,26,28); and
 - a receive client application (30) on said receiving device (24,26,28) for downloading, viewing, and/or manipulating said at least one stored document (16) from the dedicated server (22) in response to the electronic message.
2. The apparatus of Claim 1, wherein said send client application (20) further comprises a package window for specifying parameters of the document delivery.
3. The apparatus of Claim 1 or 2, wherein said send client application (20) further comprises a storage module for configurably storing said specified document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.
4. The apparatus of any of the preceding Claims, wherein said send client application (20) further comprises a module for accessing an address book from a supported application on said sending computer (14), wherein said document delivery is initiated using the contents of said address book.
5. The apparatus of any of the preceding Claims, wherein said document is delivered by selecting and dragging said document (16) onto one of an application window (32); a package window (78,180), an icon representing said send client application (20), or an icon for accessing said stored document delivery parameters.
6. The apparatus of any of the preceding claims, further comprising a Configuration User Interface (60) for involving and customizing said dedicated server (22).
7. The apparatus of Claim 6, wherein said Configuration User Interface (60) comprises:
 - a sending module for sending said document;
 - a tracking module (40,144) for tracking said document;
 - an account CUI (42,146) for accessing information associated with a document delivery account;
 - a billing module (44,148) for managing billings for said document delivery; and
 - a mail list module (46,150) for creating and managing mail distribution lists.
8. The apparatus of any of the preceding Claims, further comprising a security framework for restricting access to said apparatus and/or to said document, said security framework having at least one security module in at least one of said send client application (20), said receive client application (30), and a configuration user interface (60).
9. The apparatus of Claim 8, wherein said security framework supports at least one of authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication.
10. An apparatus for managing and delivering documents for an electronic network (18), comprising:
 - a dedicated server (22) for electronically notifying a notification receiving device on an electronic network of at least one document (16) stored on said dedicated server (22);
 - a receiving device (24,26,28) on said electronic network (18) for receiving said at least one document (16) in response to said notification; wherein said receiving device (24,26,28) uses a receive client application (30) to download said document (16) from said dedicated server (22).
11. The apparatus of Claim 10, wherein said receiving device (24,26,28) includes said notification receiving device.
12. The apparatus of Claim 10 or 11, further comprising

an HTML interface on a computer desktop (12) for managing said dedicated server (22) via a Web browser.

13. The apparatus of any of Claims 10 to 12, further comprising a send client application (20) for delivering said at least one document (16) as a single package from said desktop (12) of a sending computer (14) over said electronic network (18) during a session. 5
14. The apparatus of Claim 13, said send client application (20) comprising:
 - an application window (32,140) for displaying a send client application interface said application window (32,140) comprising a tool bar (34) for accessing main functions of said send client application (20), a package manager for listing all document activities initiated during a send client application session, and a menu listing operational commands for said send client application; 15
 - a package window (78,170) for specifying the parameters of said document delivery; and 20
 - a storage module for configurably storing said document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters. 25
15. The apparatus of any of Claims 10 to 14, further comprising a security framework for restricting access to said apparatus (10) and/or said document (16). 30
16. A method for document management and delivery on an electronic network (18) comprising the steps of: 35
 - delivering at least one document (16) as a single package from a sending computer (14) to a dedicated server (22,505) over an electronic network (18) during a session (500) using a send client application (20); 40
 - storing said at least one document (16,515) from said sending computer (14) on said dedicated server (22,505); 45
 - forwarding an electronic message to a receiving device (24,26,28,530) from said dedicated server (22,505); and 50
 - downloading said at least one stored document (535) from said dedicated server (22,505) using a receive client application (30) on said receiving device (24,26,28,530), in response to the electronic message. 55
17. The method of Claim 16, further comprising the step of:

said sending computer desktop (12) displaying an application window (32,140) with a send client application interface having a tool bar for accessing main functions of said send client application (20), a package manager for listing all document activities initiated during said session (500), and a menu listing operational commands for said send client application (20).

18. The method of Claim 17, further comprising the step of:

specifying the parameters of said document delivery in a packaging window (78,170).

19. The method of Claim 18, comprising the step of:

configurably storing, in a storage module, said specified document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.

20. The method of any of Claims 16 to 19, further comprising the step of:

providing a security framework for restricting access to said system, said security framework supporting at least one of authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication.

21. The method of any of Claims 16 to 20, further comprising the step of:

initiating said document delivery from the contents of an address book of a supported application on said sending computer (14).

22. The method of any of Claims 16 to 21, comprising the step of:

displaying a Configuration User Interface application window (140) for managing said dedicated server (22,505) on a computer desktop (12), said configuration user interface application window (140) having a main tool bar for accessing main functions of said configuration user interface, a secondary tool bar for accessing functions within said main functions, a workspace for displaying an interactive interface to an accessed function, and a menu listing operational commands for said configuration user interface.

23. An apparatus for generating a digital certificate (1345) for a recipient (1370) by a sender (1352),

comprising:

a sending computer (1352) for use by said sender;
 a receiving computer (1370) for use by said recipient;
 a database (1346) for storing recipient information;
 means for gathering information from said recipient (1370); and
 means for controllably generating a digital certificate (1345) for said recipient (1370) if said gathered information and said stored recipient information match.

24. The apparatus of Claim 23, further comprising:

- means for querying said database (1346) by said sender (1352) for said stored recipient information;
- means for comparing said gathered private recipient information and said stored recipient information;
- means for storing said digital certificate (1345); and
- means for transferring said public key (1332) to said sending computer (1352); and wherein said means for controllably generating a digital certificate (1345) comprising a public key (1332) and a private key (1340) at said receiving computer (1370).

25. The apparatus of Claim 23 or 24, further comprising:

a server (1358) interposed between said sending computer (1352) and said receiving computer (1370).

26. The apparatus of Claim 25, wherein said database (1346) for storing recipient information is located on said server (1358).

27. The apparatus of Claim 25 or 26, wherein said means for querying said database (1346) by said sender (1352) for said stored recipient information is located on said server (1358).

28. The apparatus of any of Claims 25 to 27, wherein said means for gathering information from said recipient (1370) is located on said server (1358).

29. The apparatus of any of Claims 25 to 28, wherein said means for comparing said gathered private recipient information and said stored recipient information is located on said server (1358).

30. The apparatus of any of Claims 25 to 29, wherein

said means for storing said digital certificate (1345) is located on said server (1358).

31. The apparatus of any of Claims 25 to 30, wherein said means for controllably generating a digital certificate (1345) is located on said server (1358).

32. The apparatus of any of Claims 25 to 31, wherein said means for controllably generating a digital certificate (1345) includes software that is downloadable from said server (1358) to said receiving computer (1370).

33. The apparatus of any of Claims 23 to 32, further comprising:

a certificate digest comprising said stored recipient information and sender selectable options for said digital certificate (1345).

34. A method for generating a digital certificate for a recipient by a sender (1352), comprising the steps of:

querying a database (1346) for stored recipient information;
 gathering information from said recipient (1370);
 comparing said gathered information with said queried, stored recipient information;
 selectively transferring software to said recipient based upon said comparison; and
 selectively generating said digital certificate (1345) at said recipient with said software, said digital certificate (1345) comprising a public key (1332) and a private key (1340).

35. The method of Claim 34, further comprising the step of: transferring a copy of said digital certificate (1345) to said sender (1352).

36. The method of Claim 34 or 35, further comprising the step of: transferring a copy of said public key (1332) to said sender (1352).

37. The method of any of Claims 34 to 36, wherein said database (1346) for storing recipient information is located on a server (1358, 1362, 1380).

38. The method of any of Claims 34 to 37, wherein said step of querying said database (1346) is performed by a server (1358, 1362, 1388).

39. The method of any of Claims 34 to 38, wherein said step of gathering information from said recipient (1370) is performed by a server (1358, 1362, 1388).

40. The method of any of Claims 34 to 39, wherein said

step of comparing said gathered information with said queried, stored recipient information (1348) is performed by a server (1358,1362,1388).

41. The method of any of Claims 34 to 40, further comprising the step of:

generating a certificate digest (1347) comprising said stored recipient information (1348) and sender selectable options (1349) for said digital certificate (1345).

15

20

25

30

35

40

45

50

55

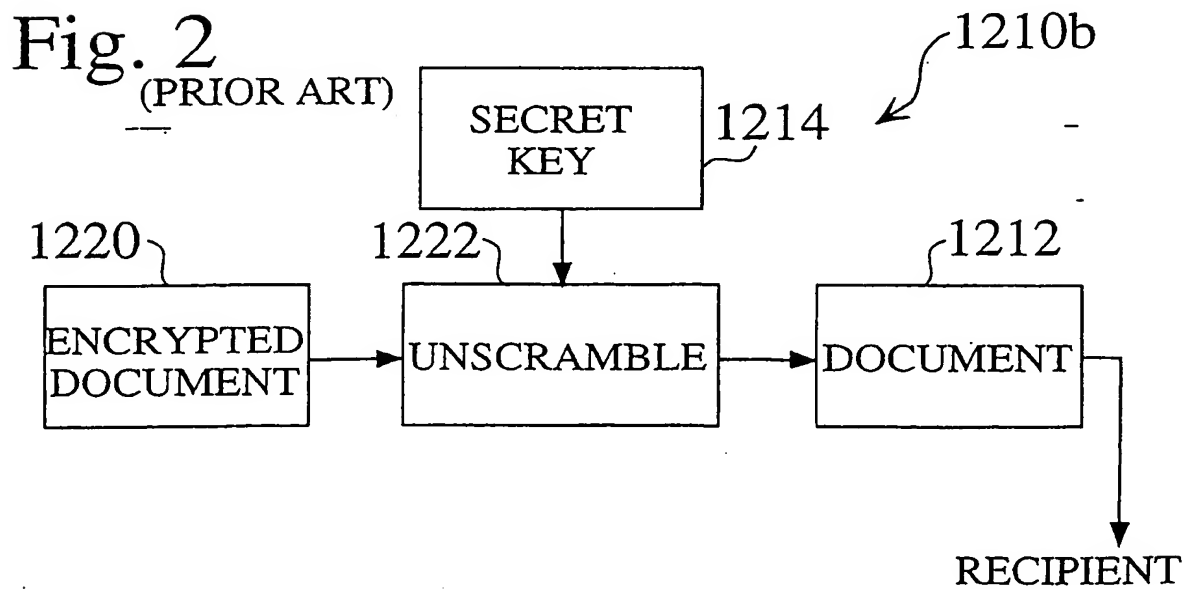
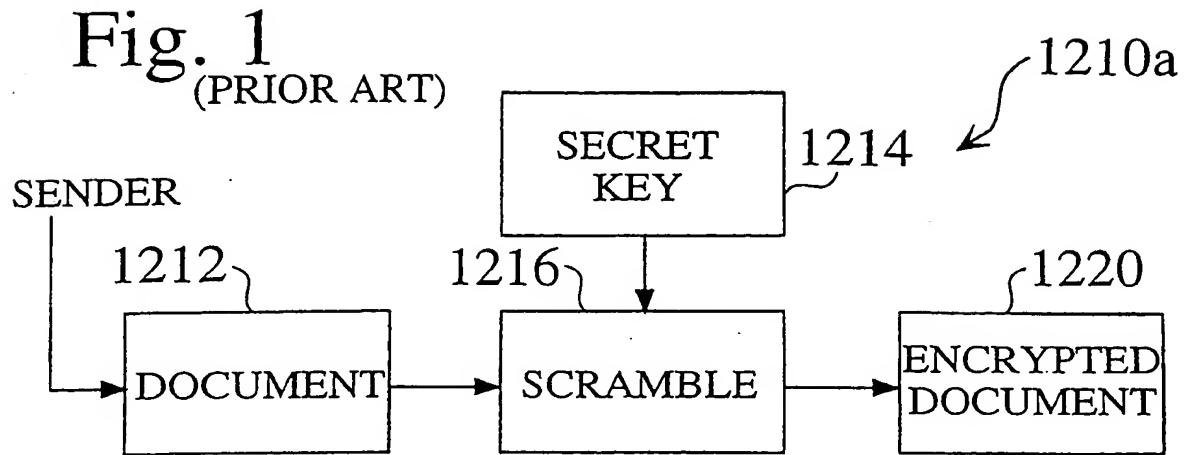


Fig. 3

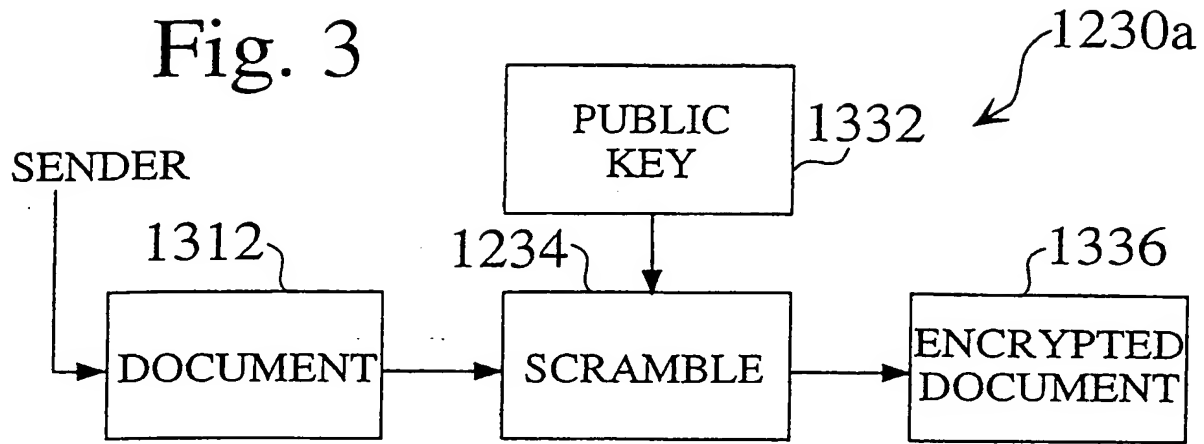
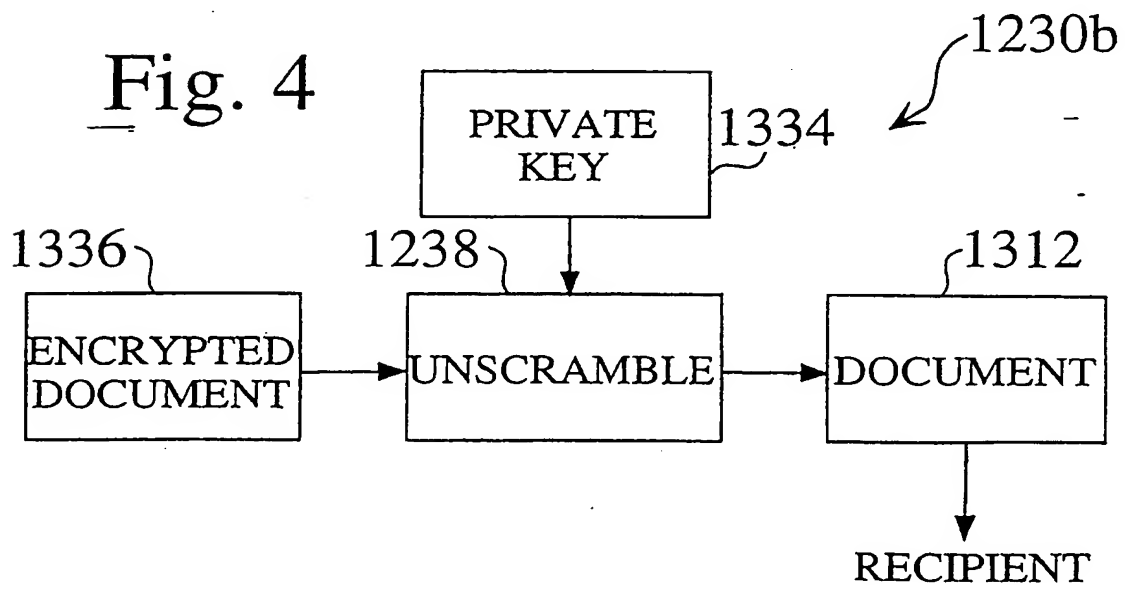


Fig. 4



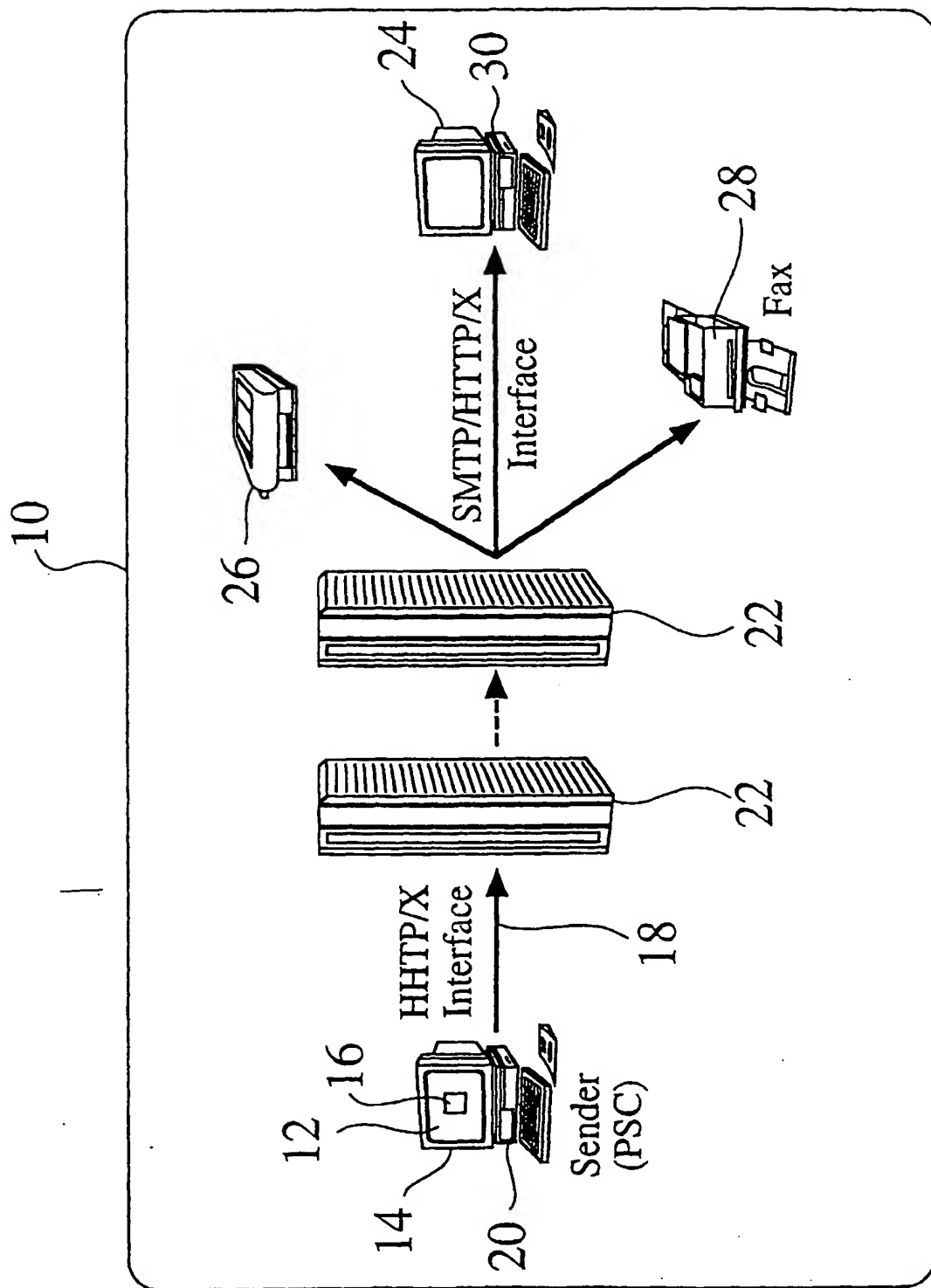


Fig. 5

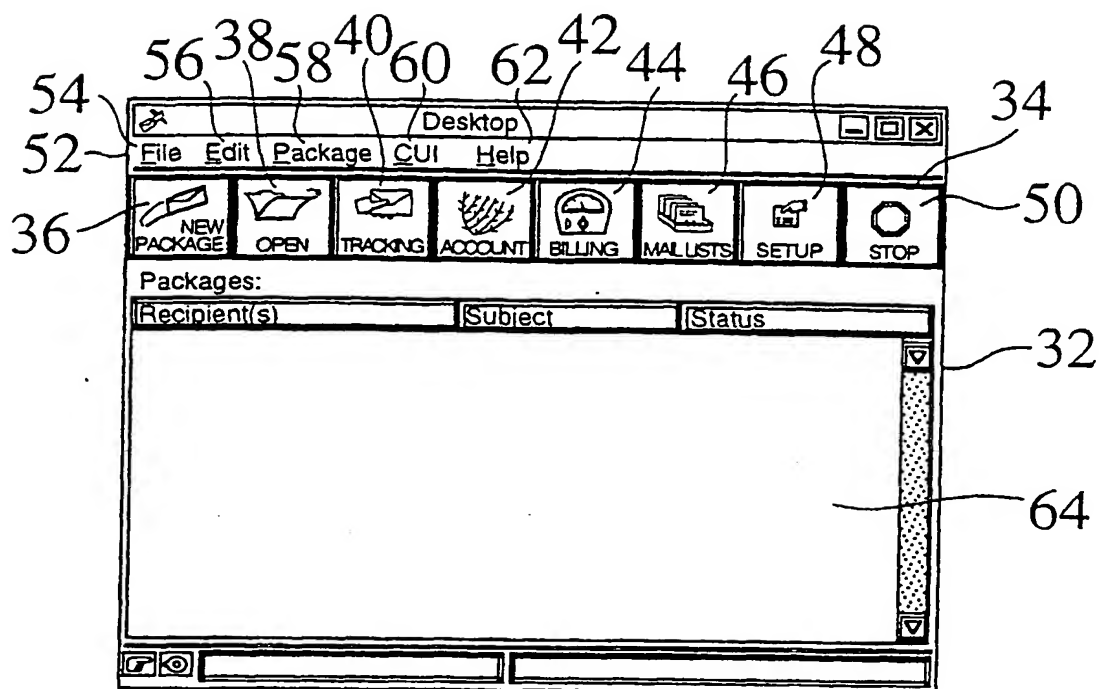


Fig. 6

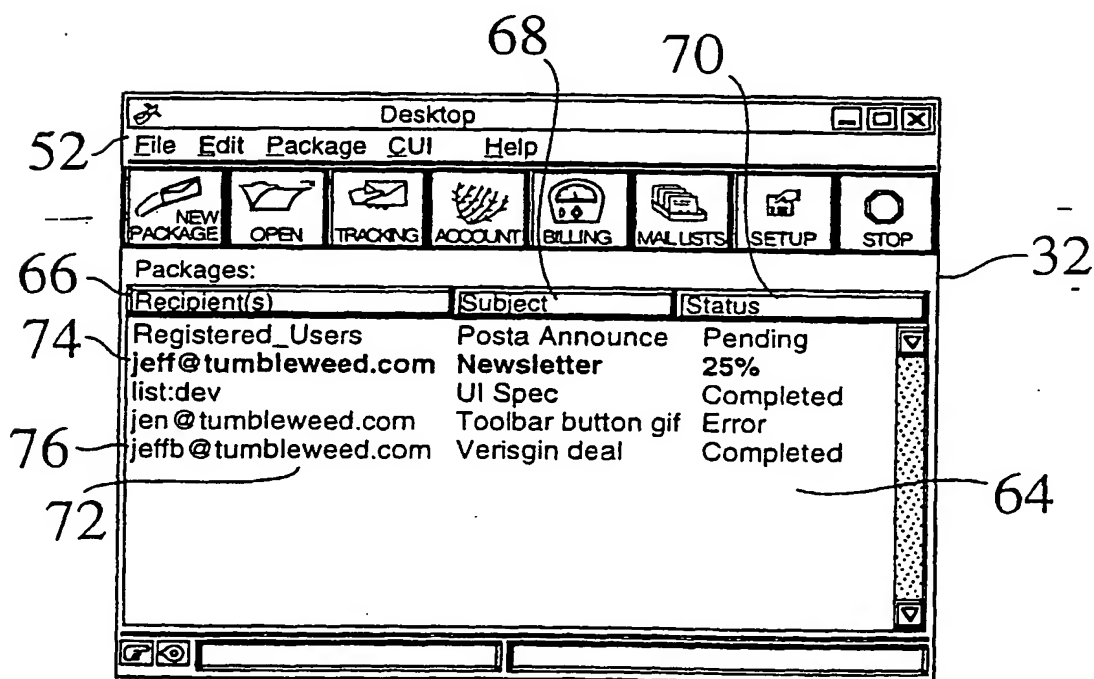


Fig. 7

The form is titled "No Subject" and is divided into several sections:

- Recipients:** Contains a "To:" field (110).
- Contents:** Contains a "Subject:" field (134) and a "Message:" field (136).
- Documents:** Contains a "File name" field (84), a "Size" field (112), and a "File format" dropdown menu (114) set to "Original".
- Priority and Confirmation:** Contains a "Priority" dropdown menu (80) set to "Normal", a "Request confirmation" checkbox (82), a "Security" section (100) with "Password:" (102) and "Confirm Password:" (104) fields, an "Encrypt document" checkbox (106), a "Require SSL to receive" checkbox (106), a "Document expiration" field (86) set to "10" days, a "Scheduled notification" field (88) set to "Thurs Mar 20, 1997" at "1:00 PM", and a "Billing Code" field (90) set to "none".
- Buttons:** Includes "Clear form" (92), "Save form" (94), "Save as Parameter" (96), "SEND" (98), "Refresh" (114), and "Save settings as default" (116).

Fig. 8

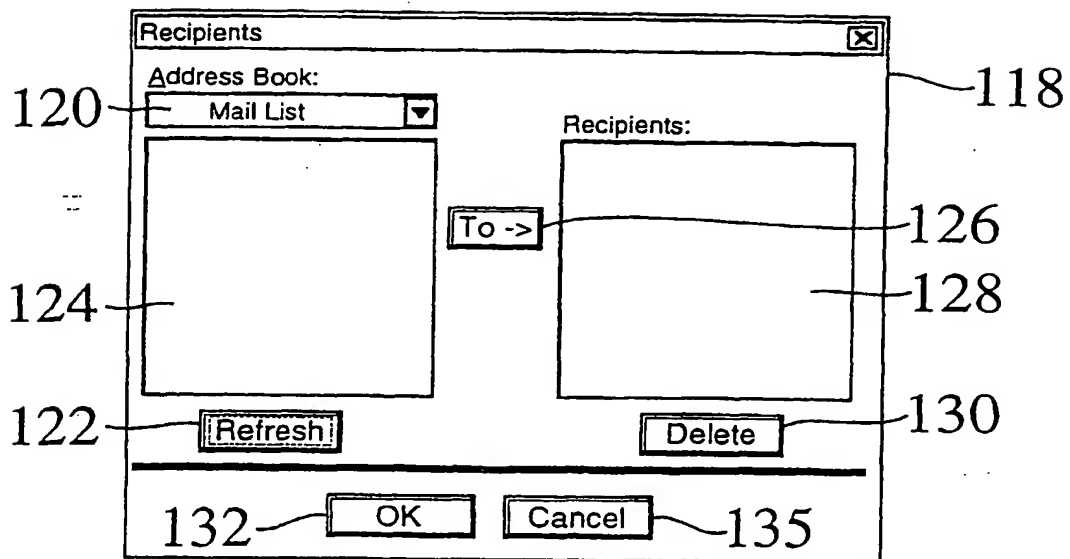


Fig. 9

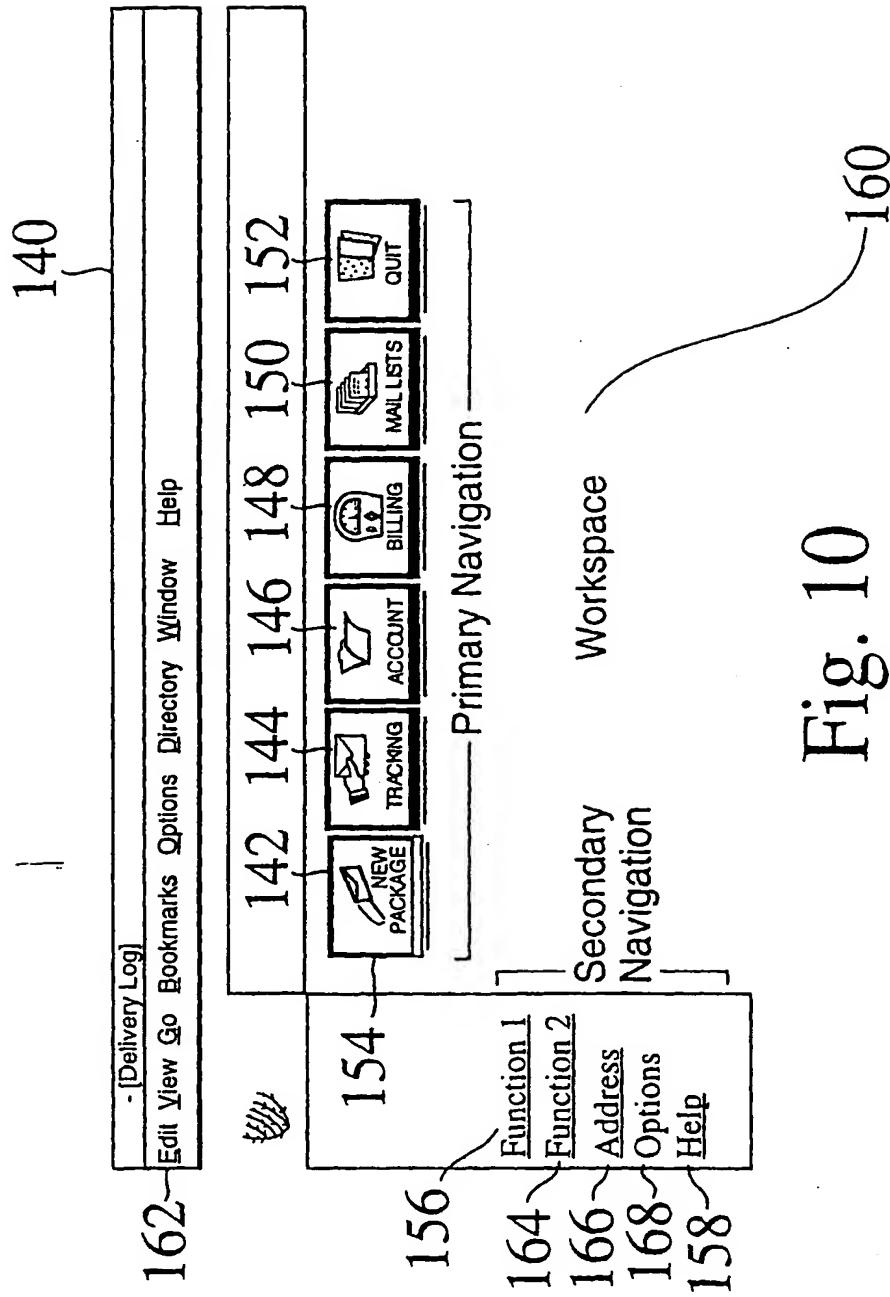


Fig. 10

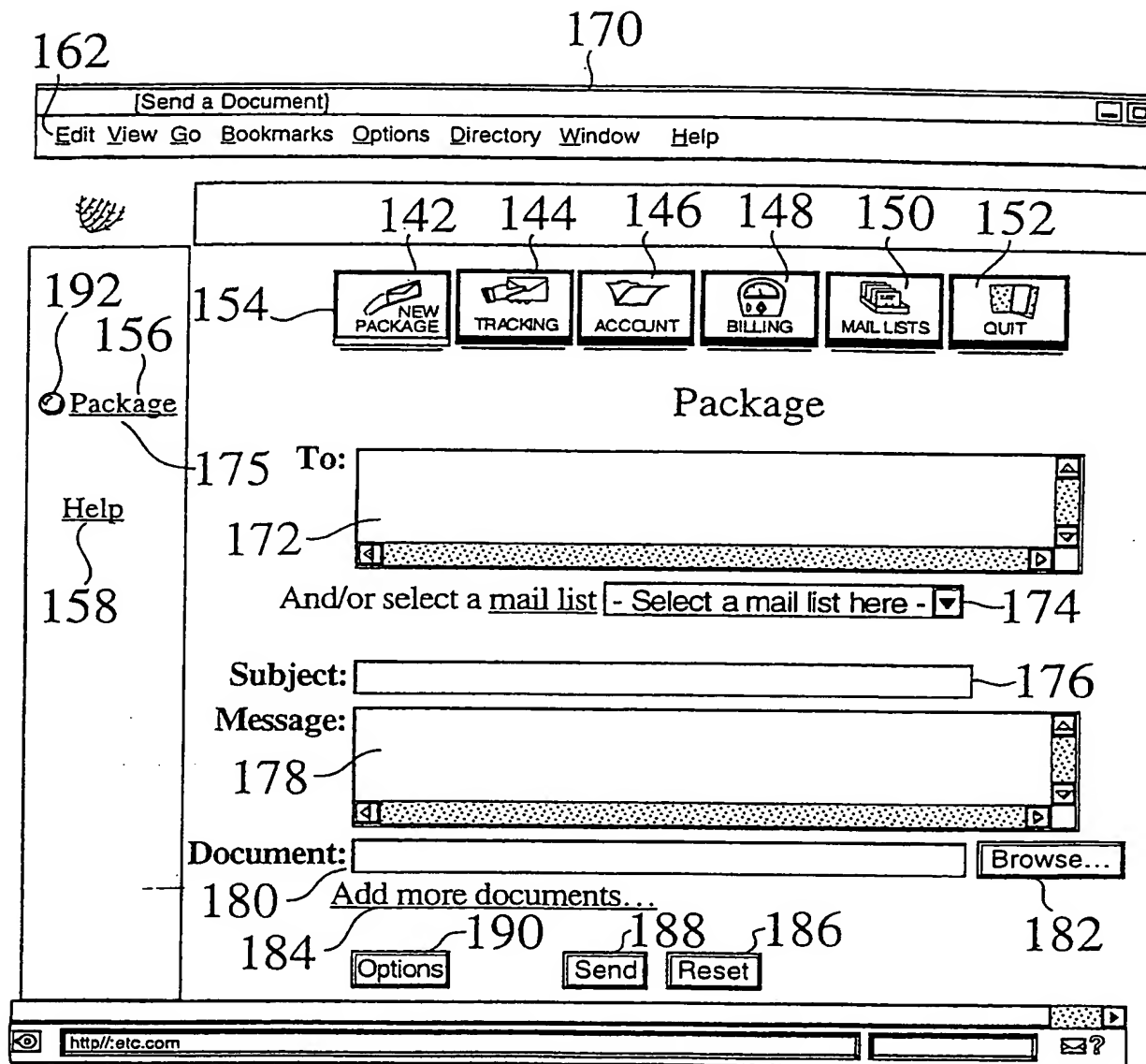


Fig. 11

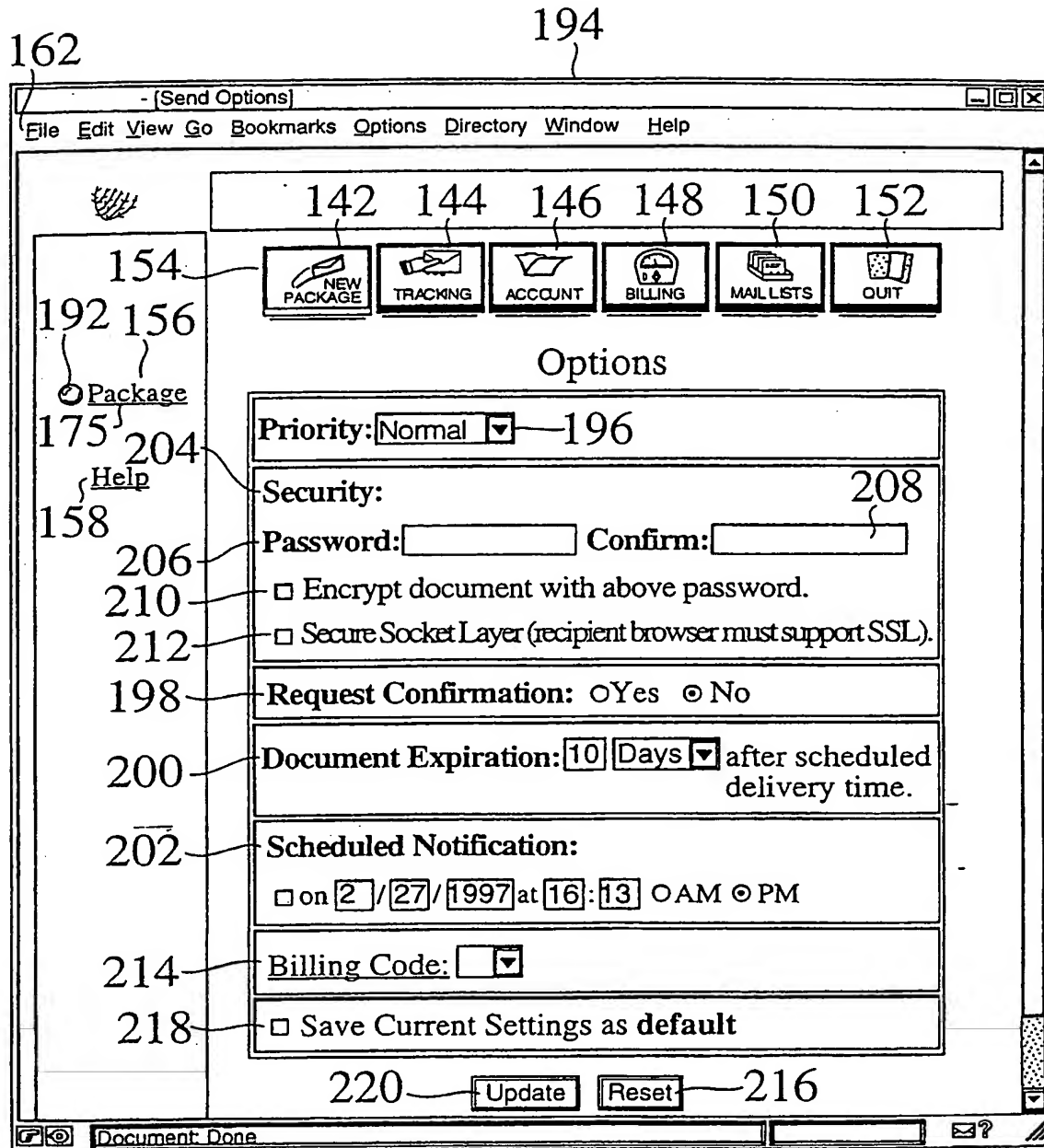


Fig. 12

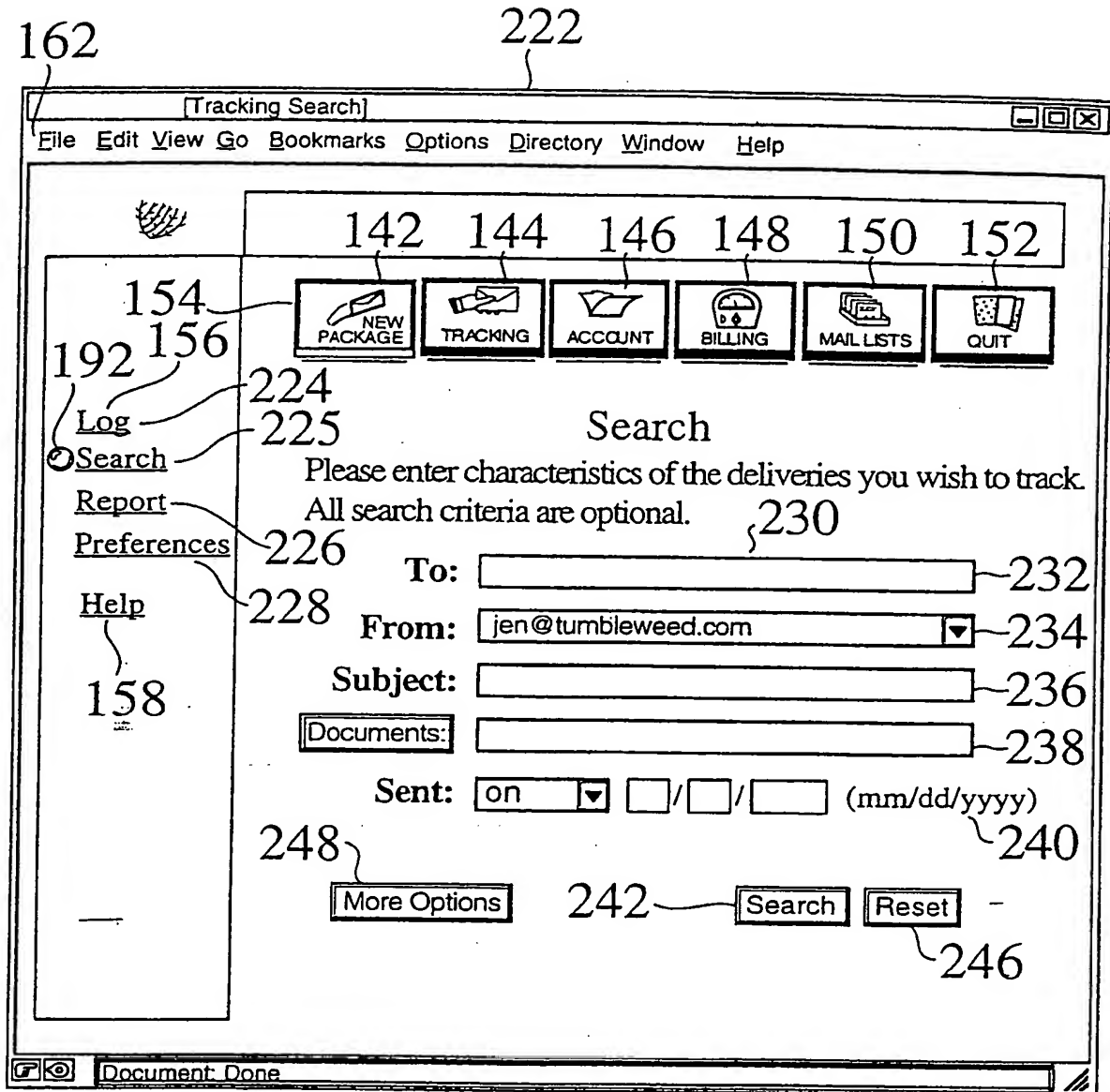


Fig. 13

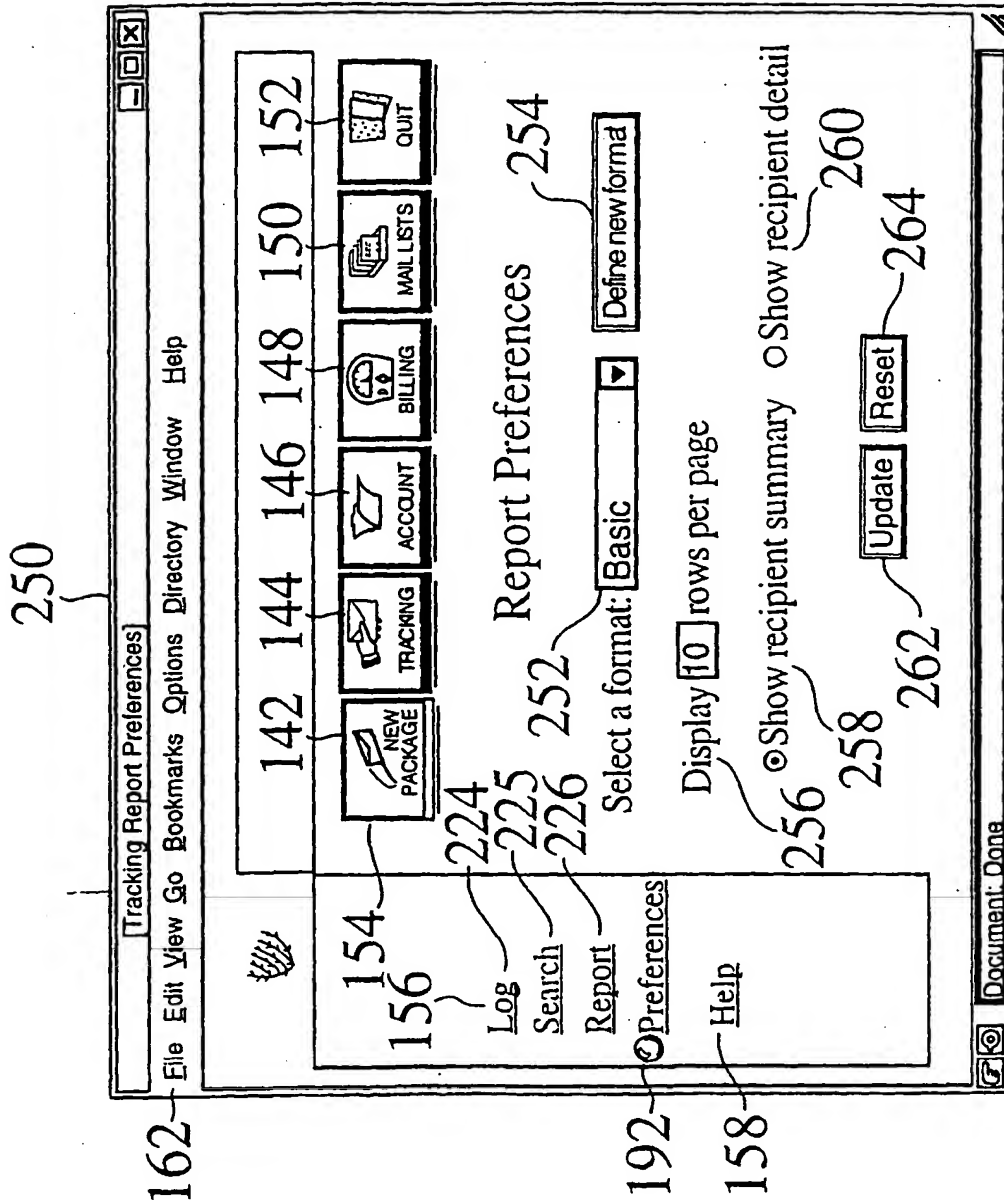


Fig. 14

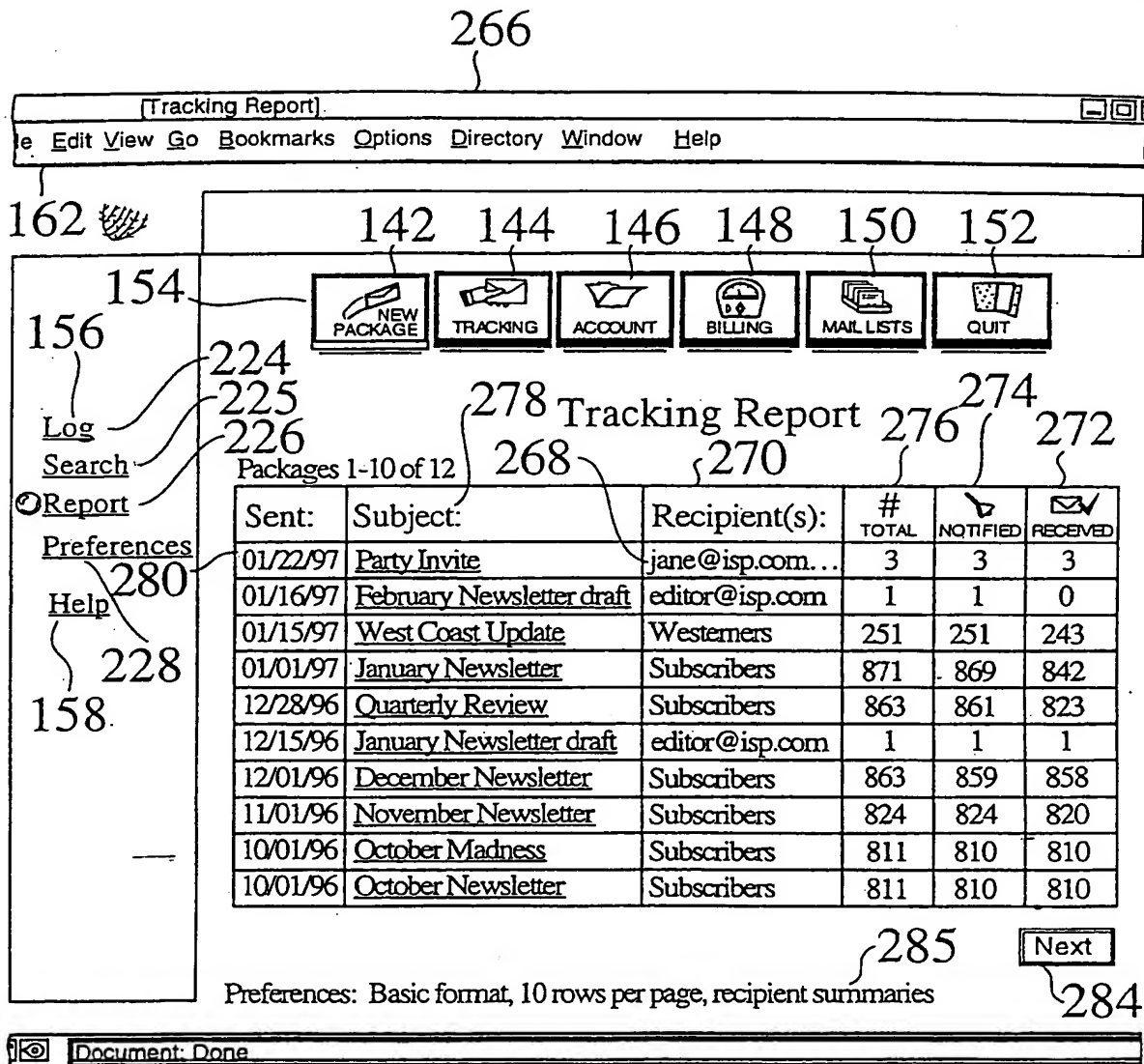


Fig. 15

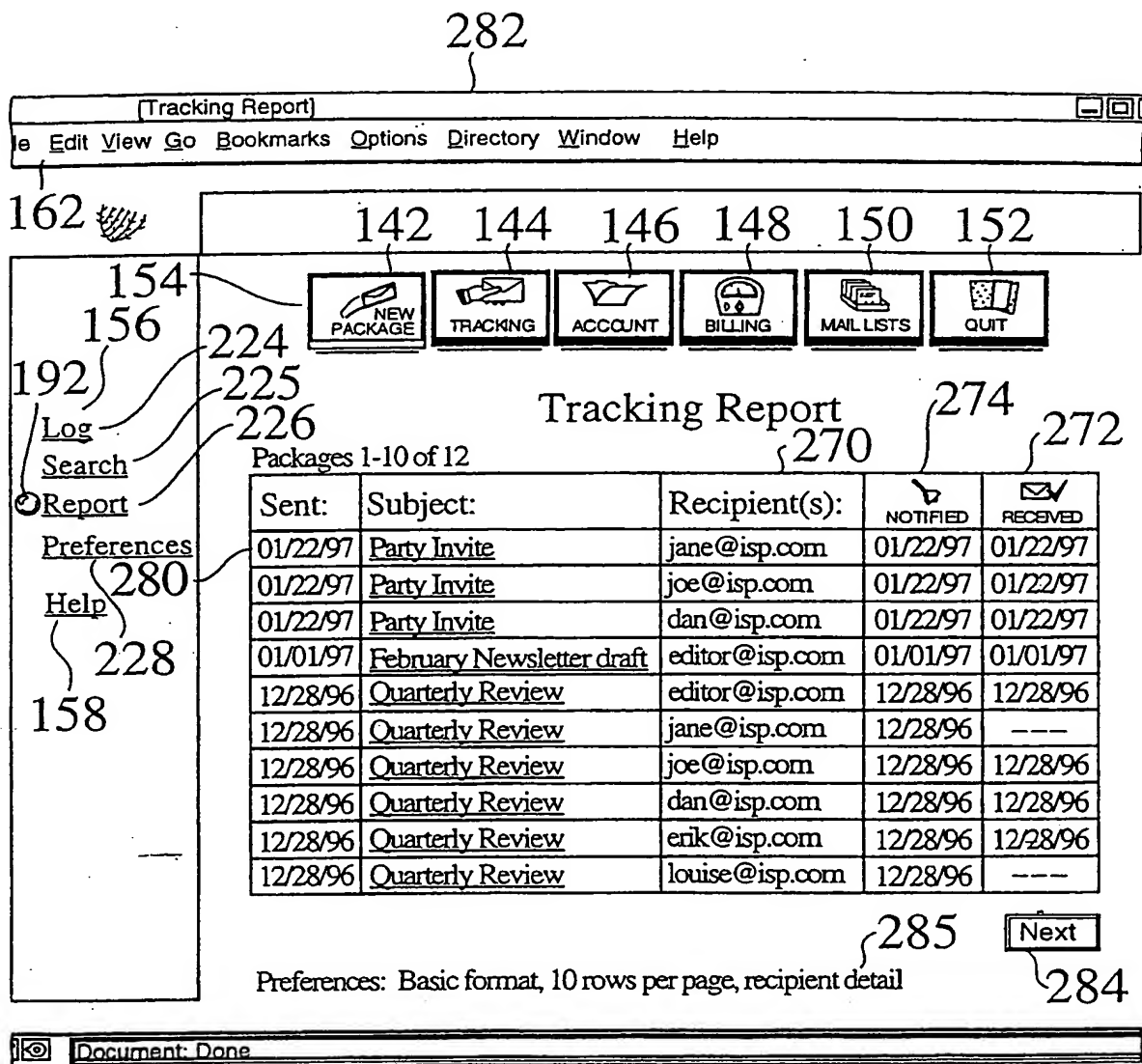


Fig. 16

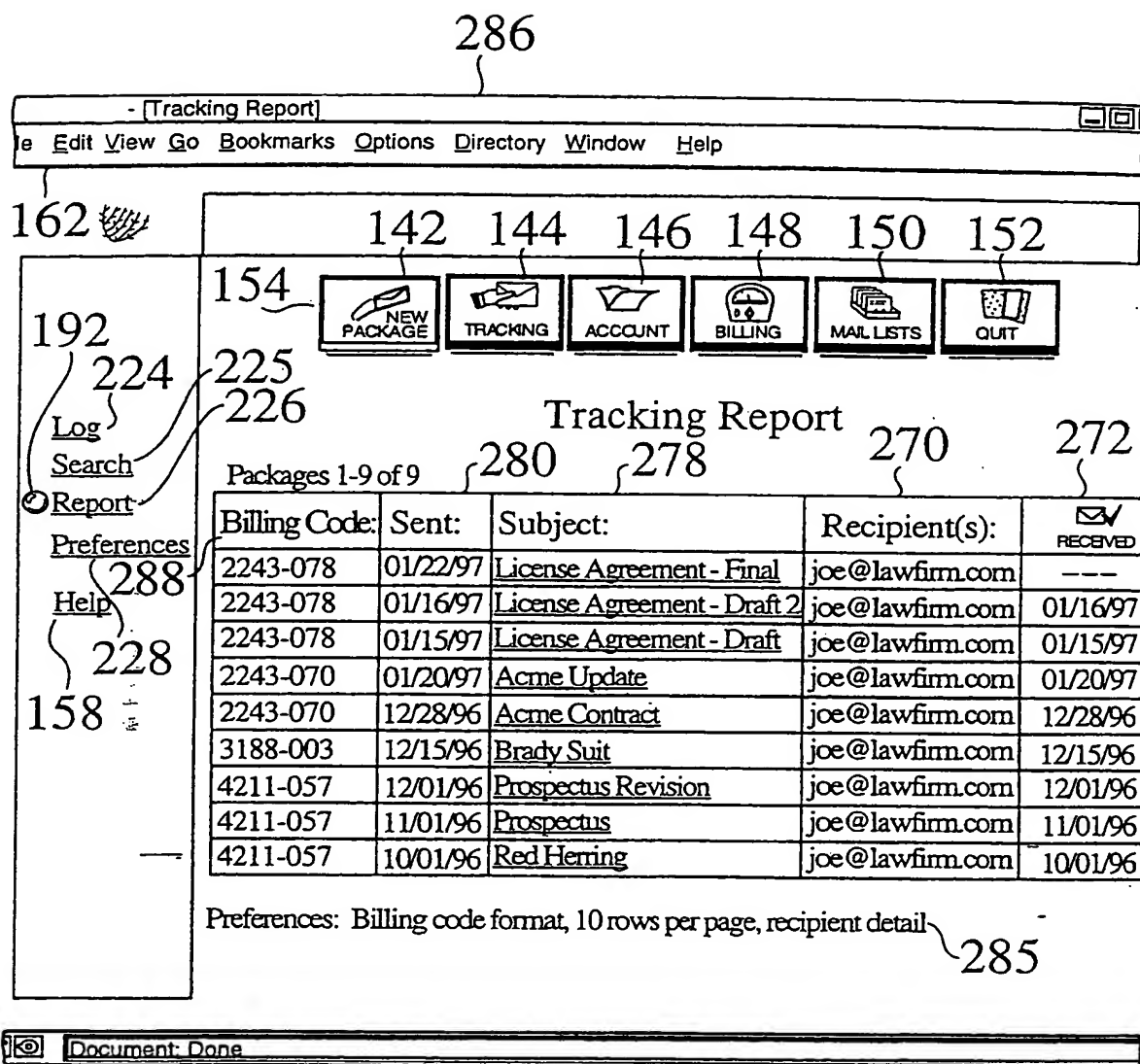


Fig. 17

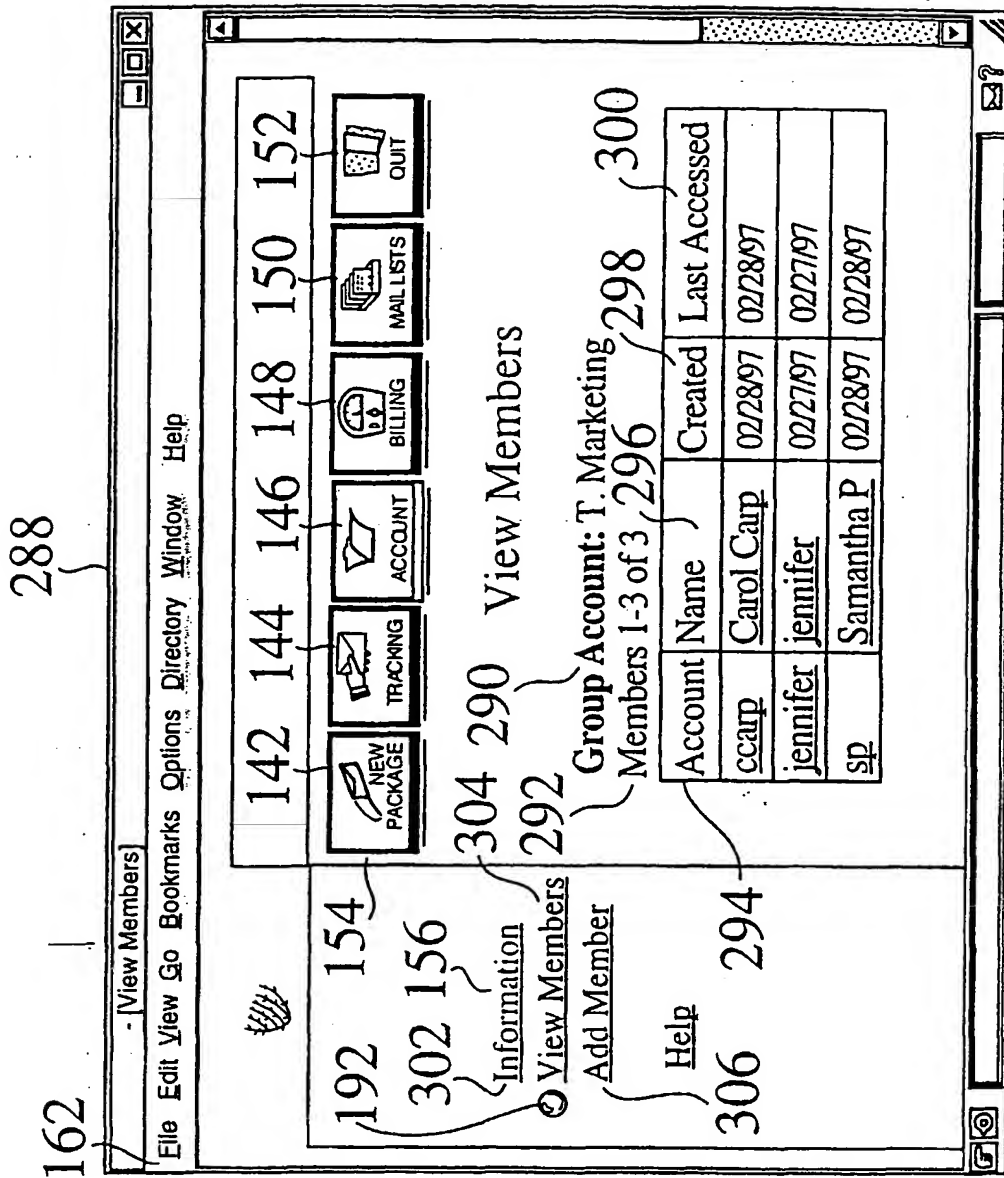


Fig. 18

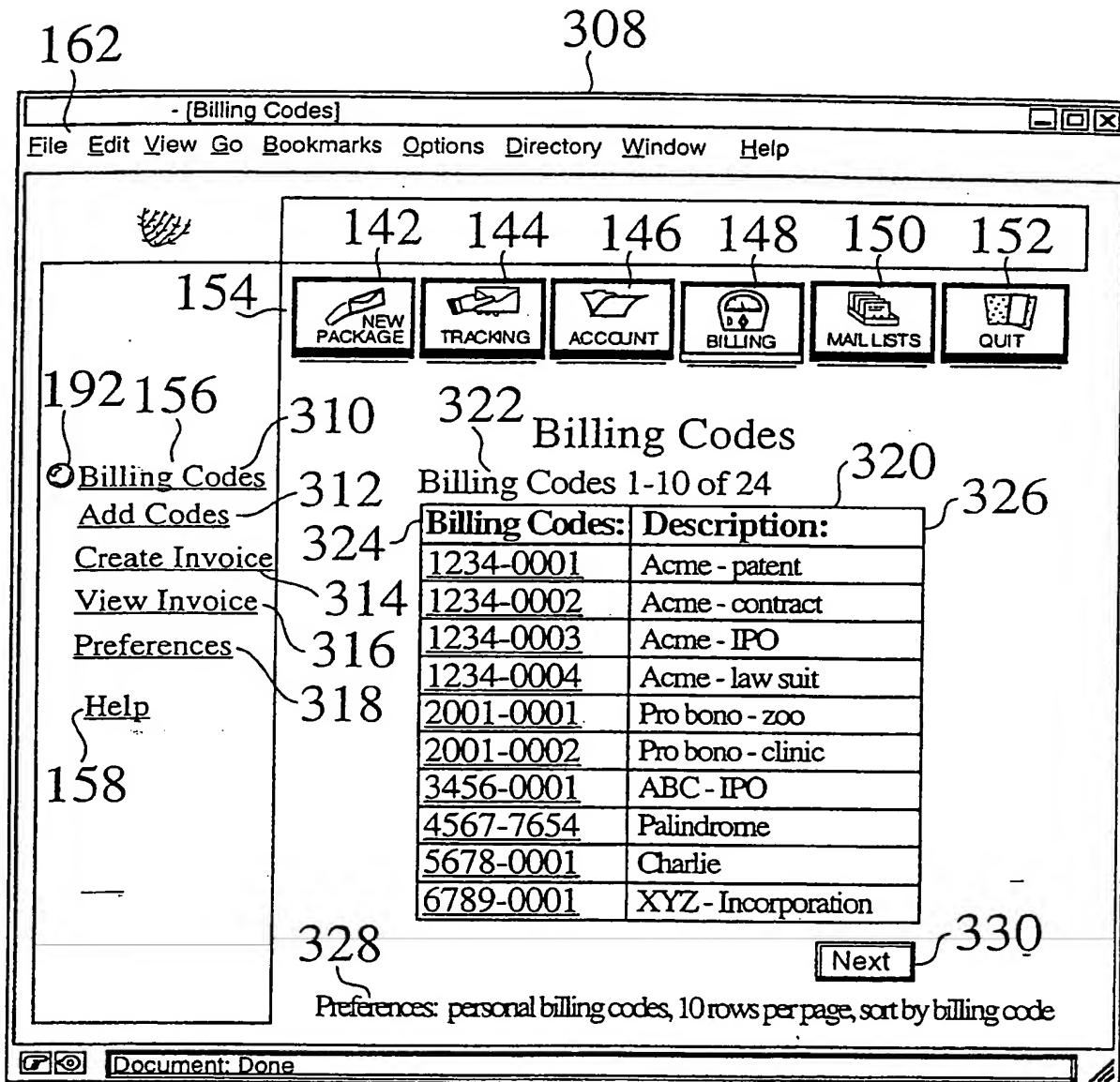


Fig. 19

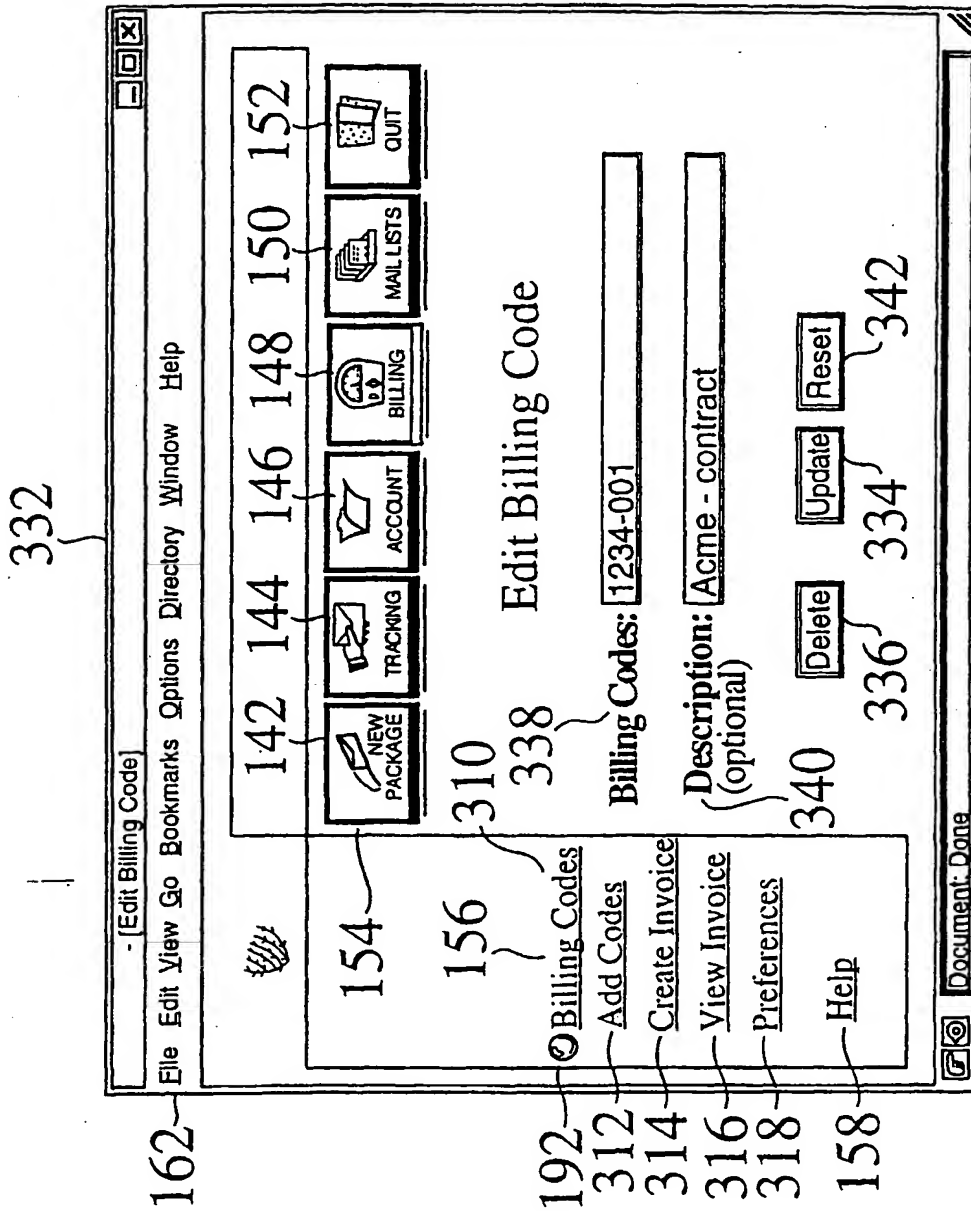


Fig. 20

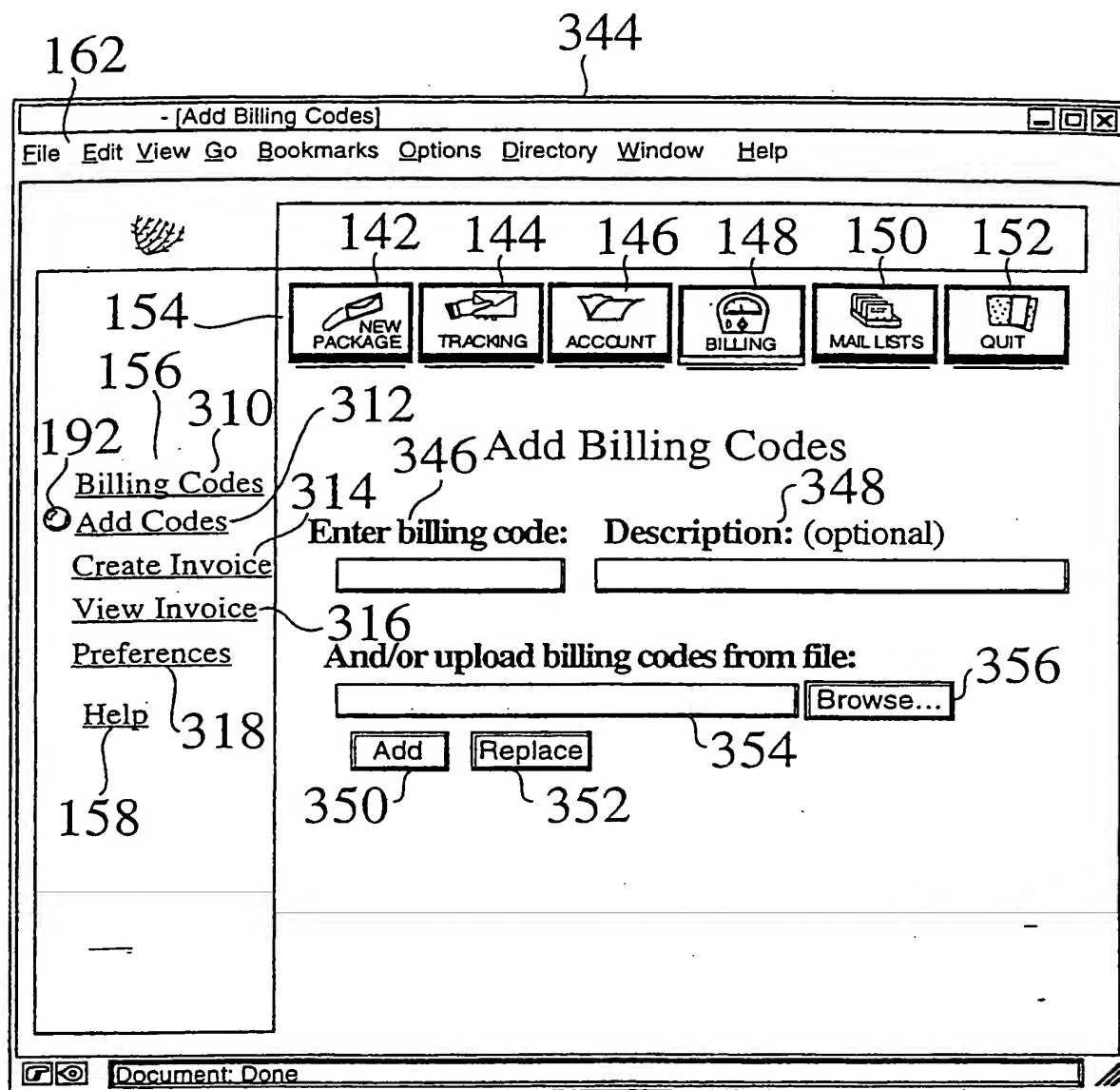


Fig. 21

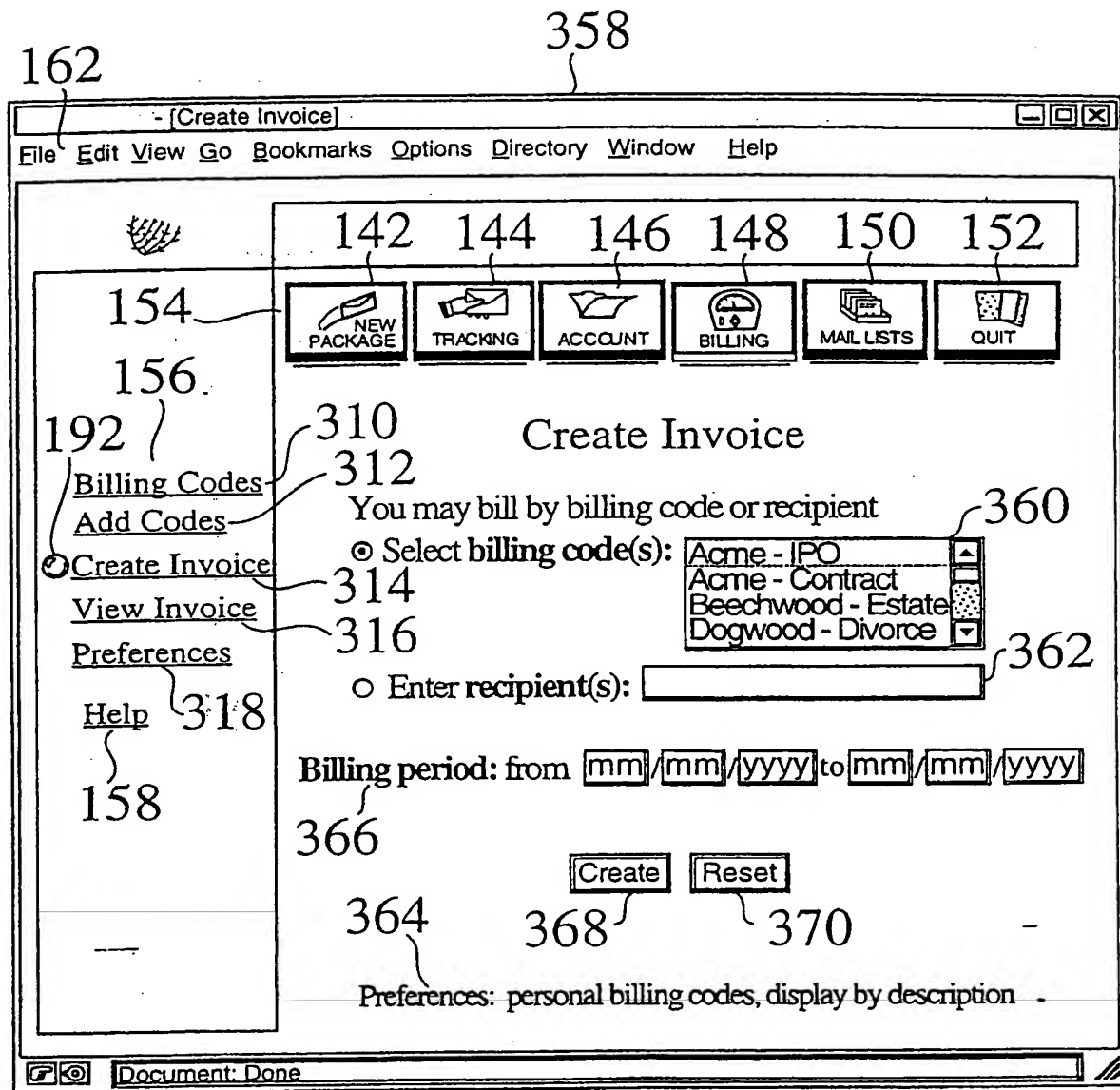


Fig. 22

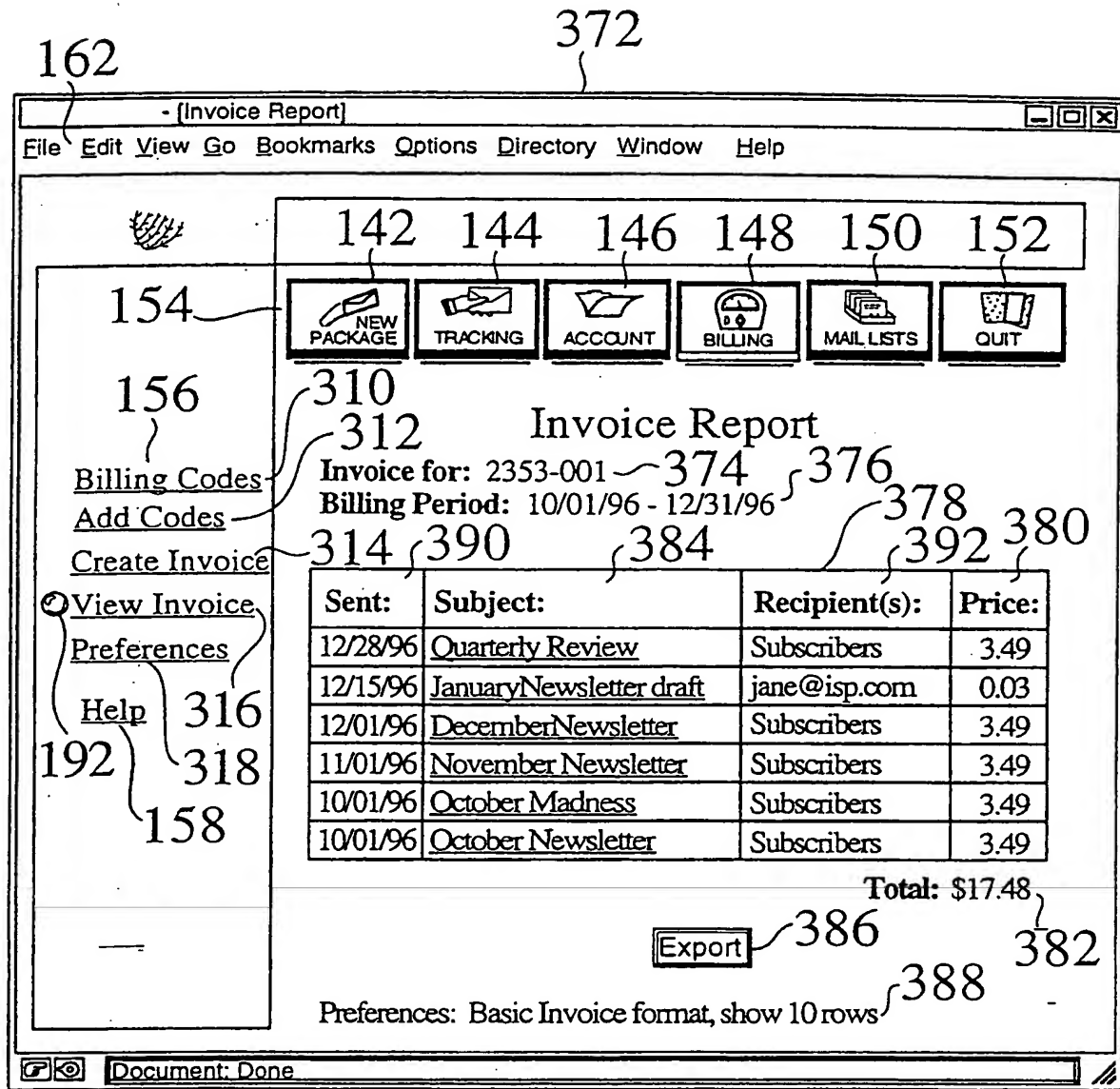


Fig. 23

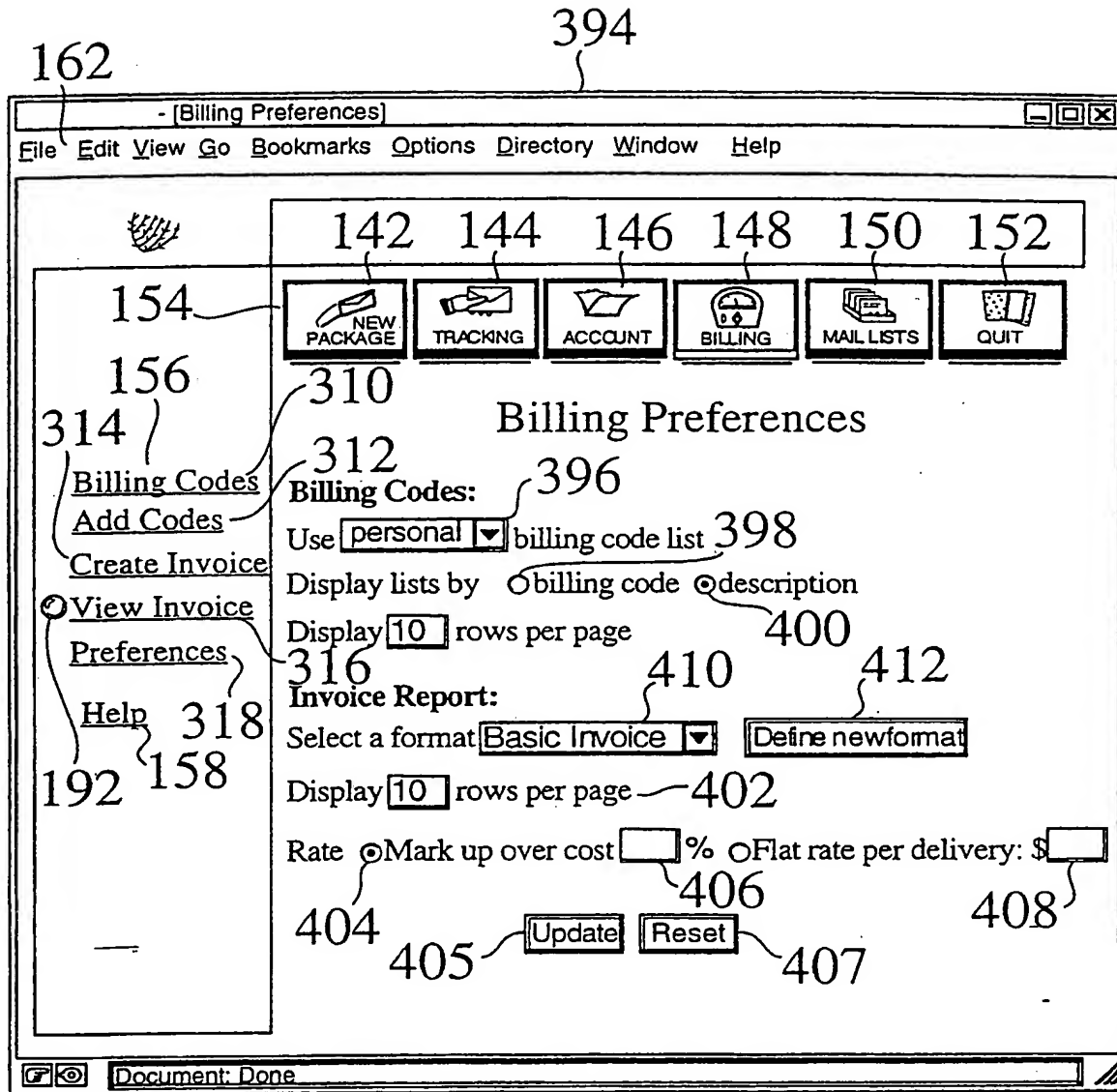


Fig. 24

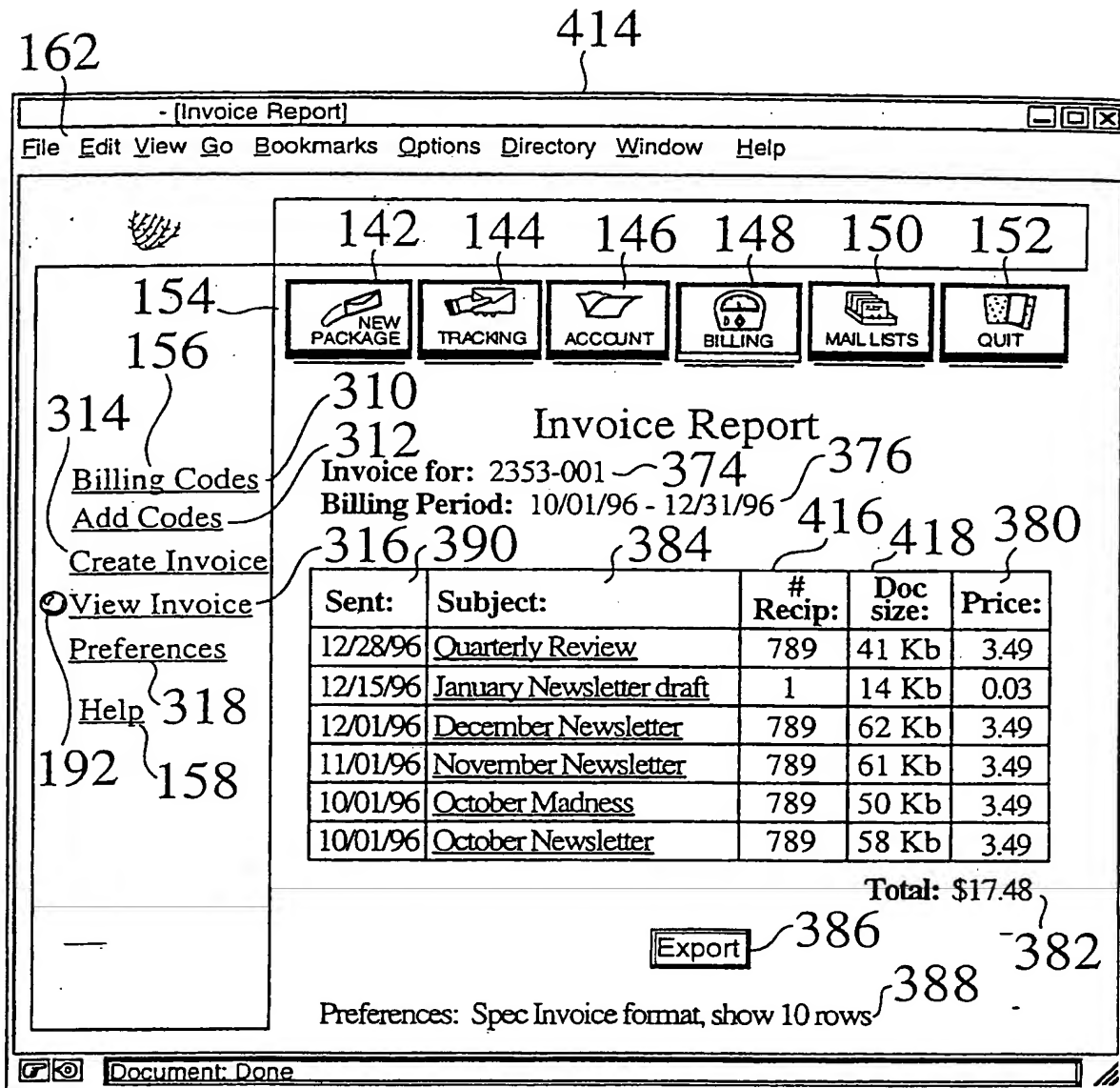


Fig. 25

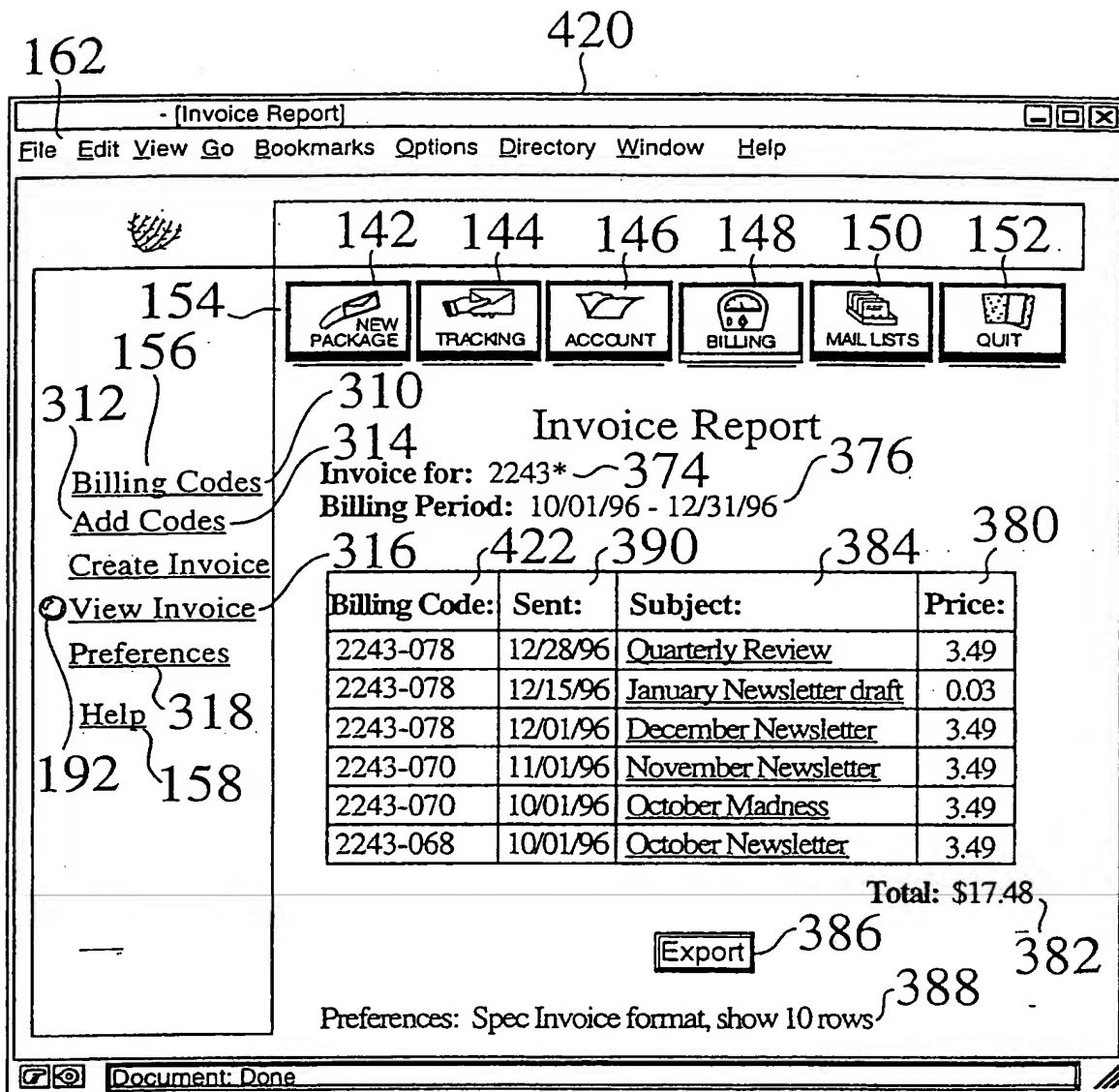


Fig. 26

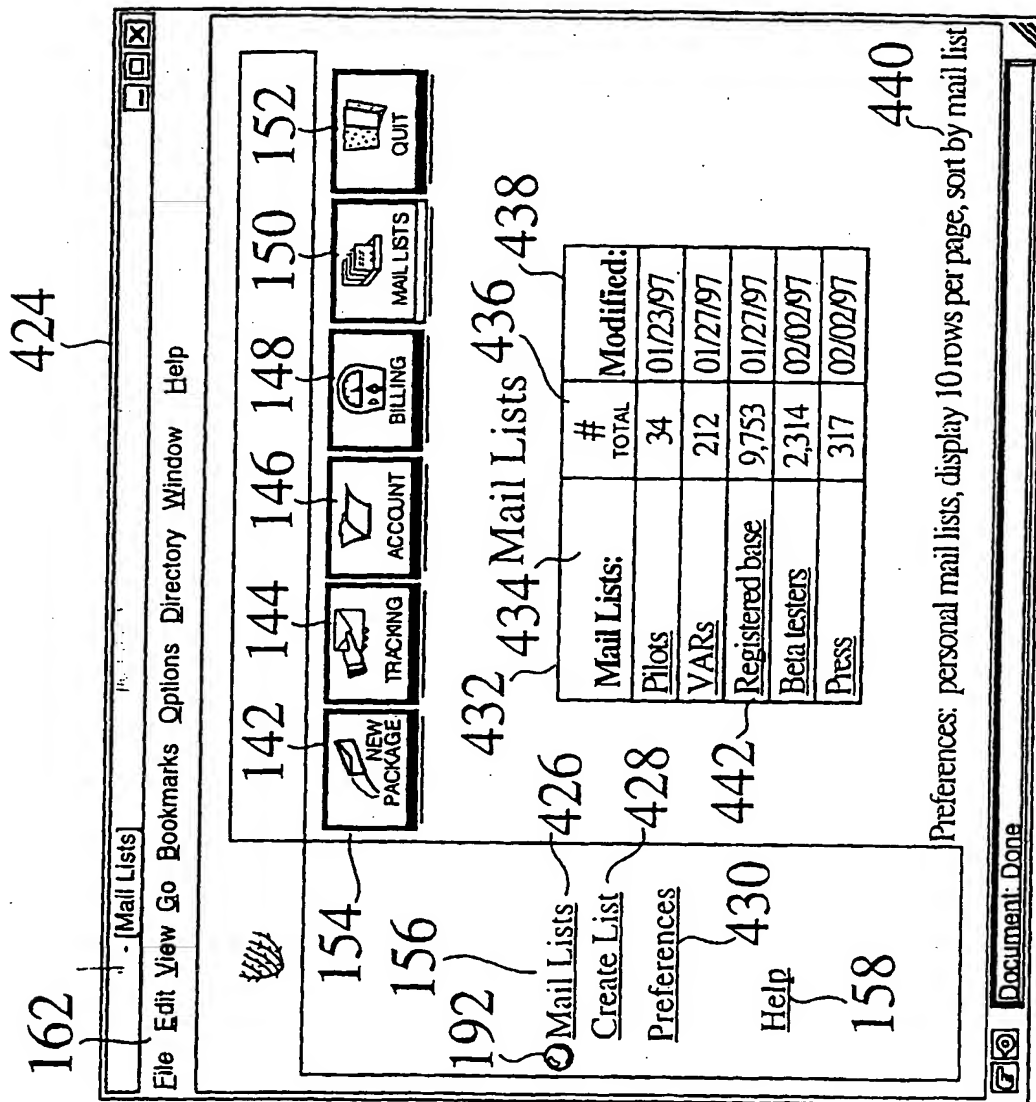


Fig. 27

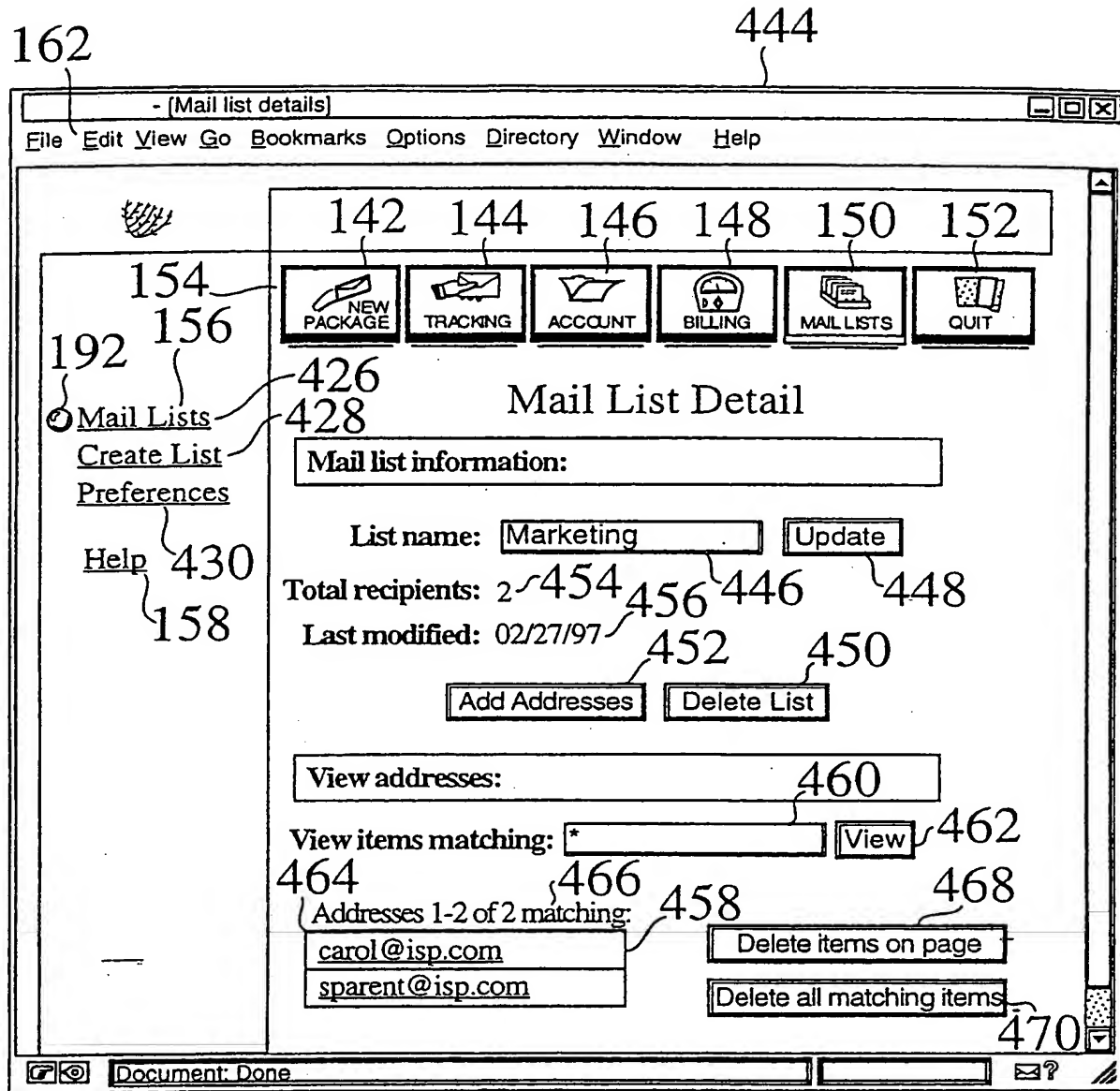


Fig. 28

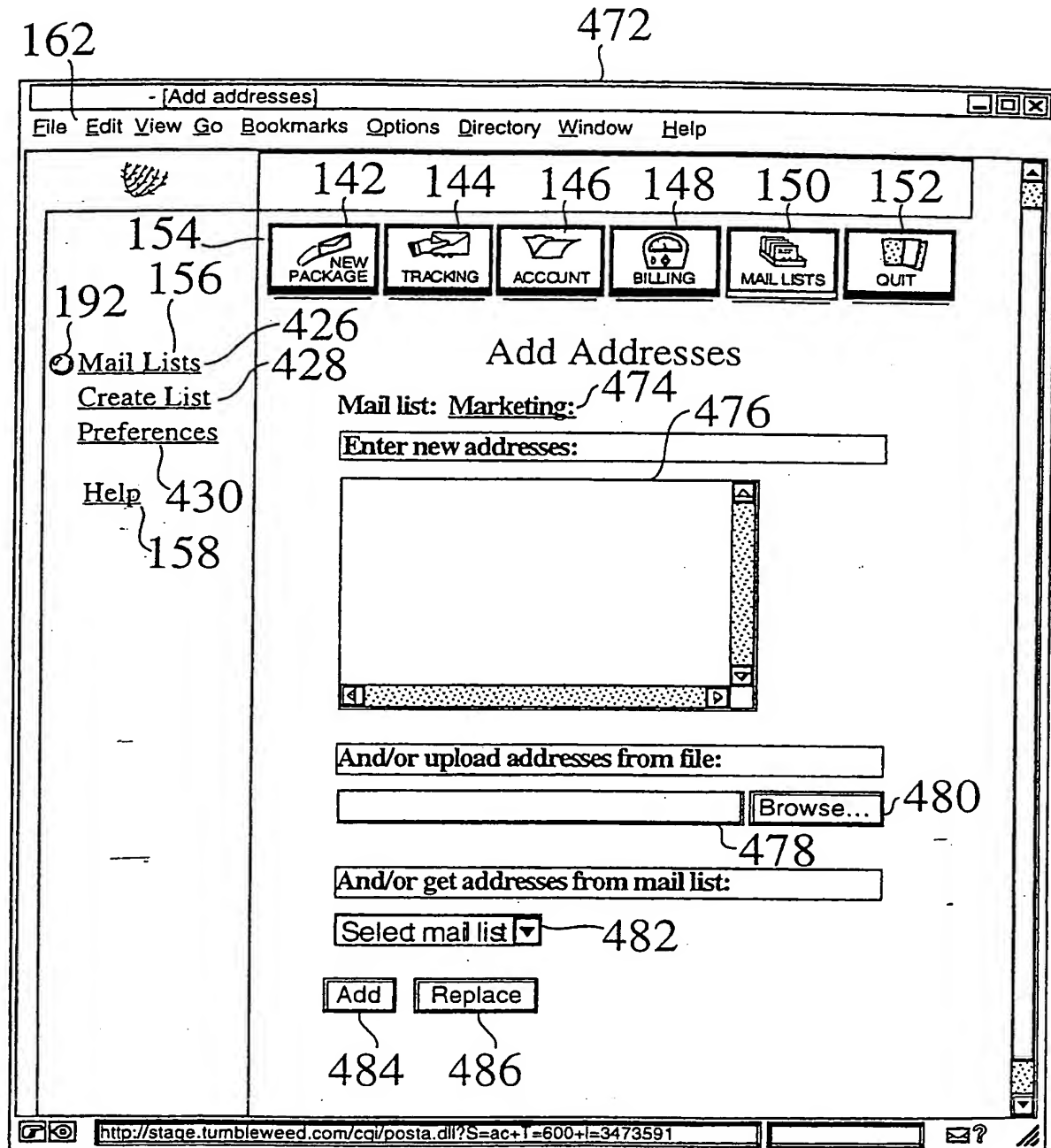


Fig. 29

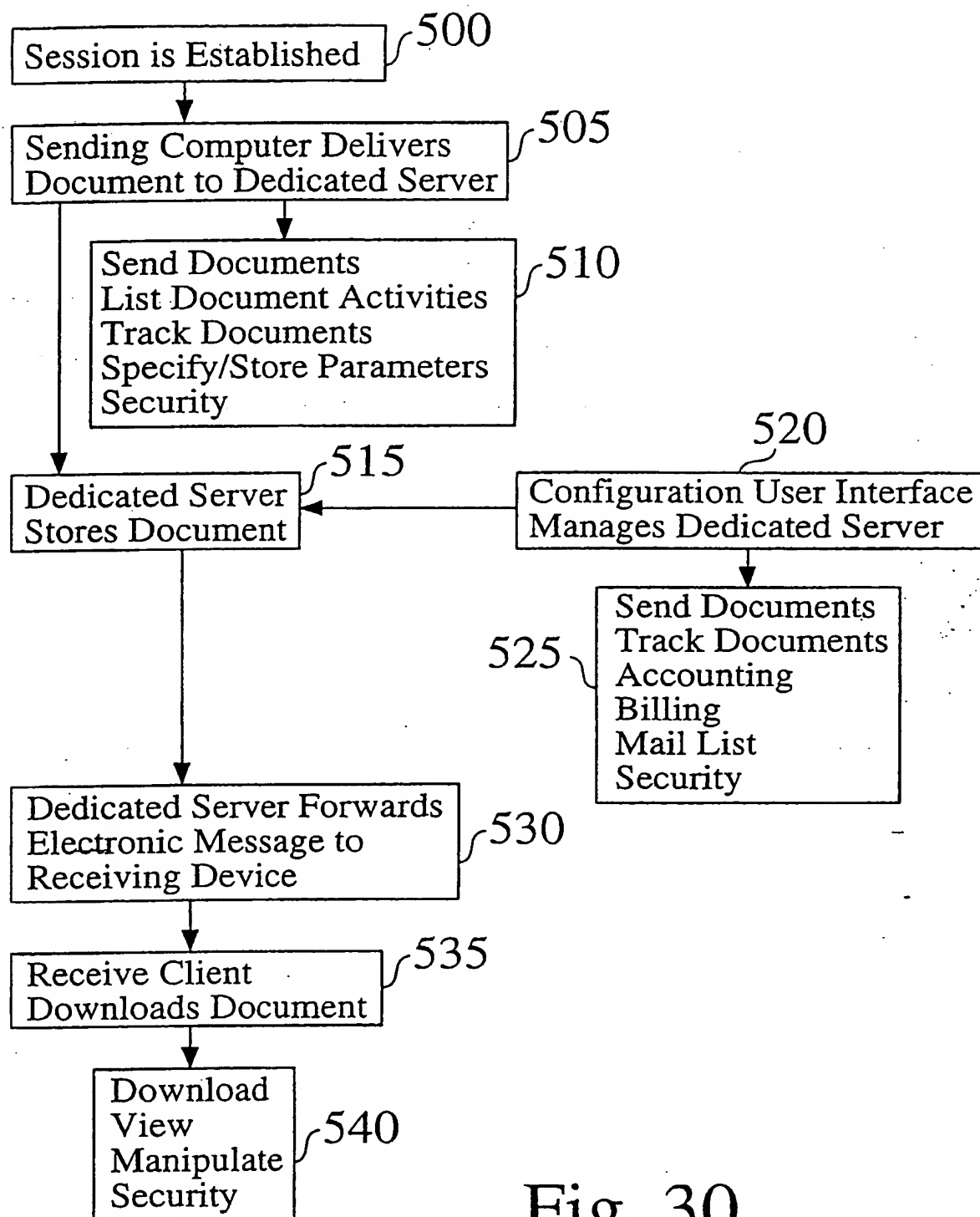


Fig. 30

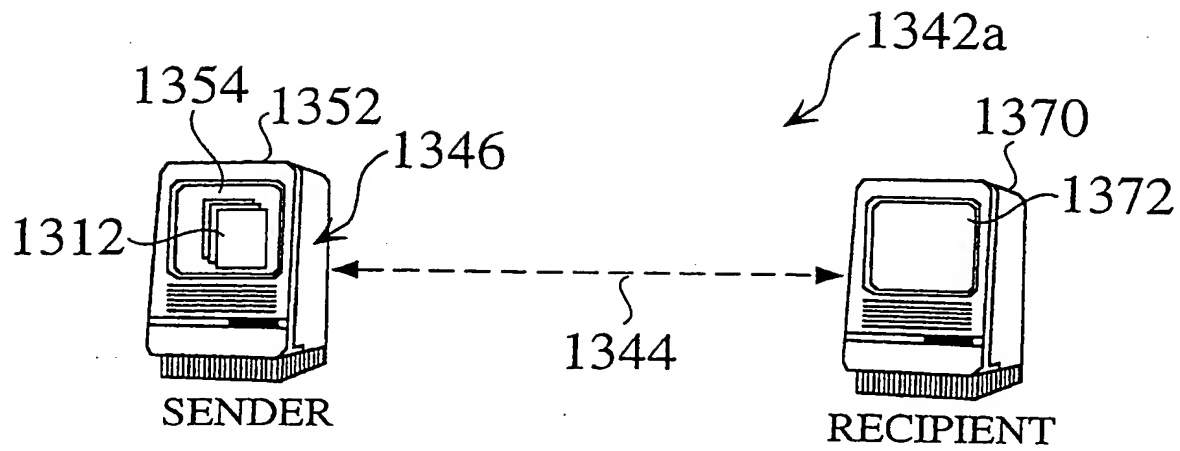


Fig. 31

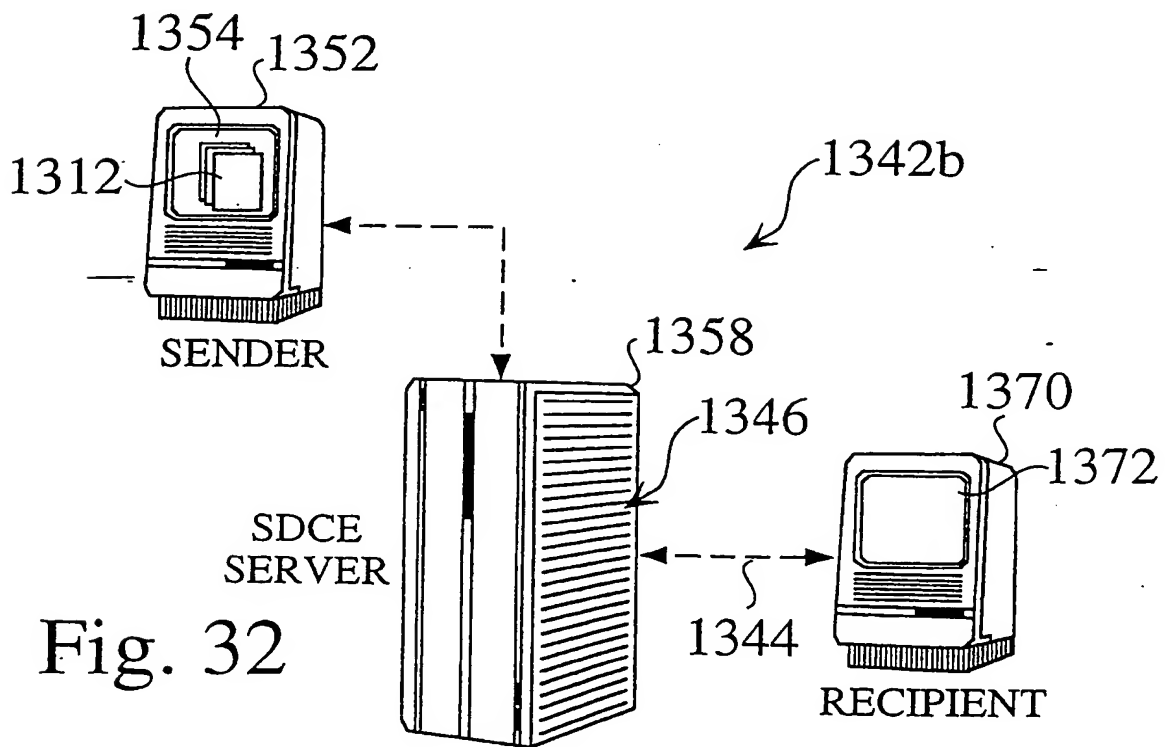


Fig. 32

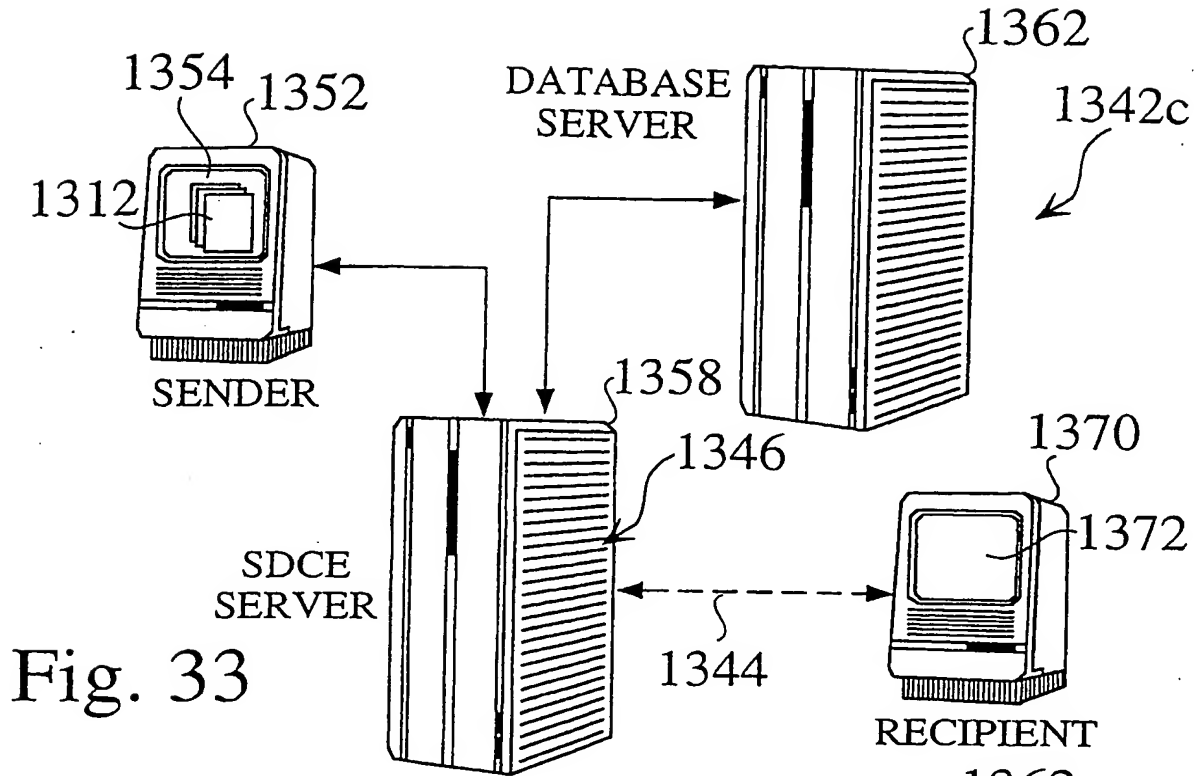


Fig. 33

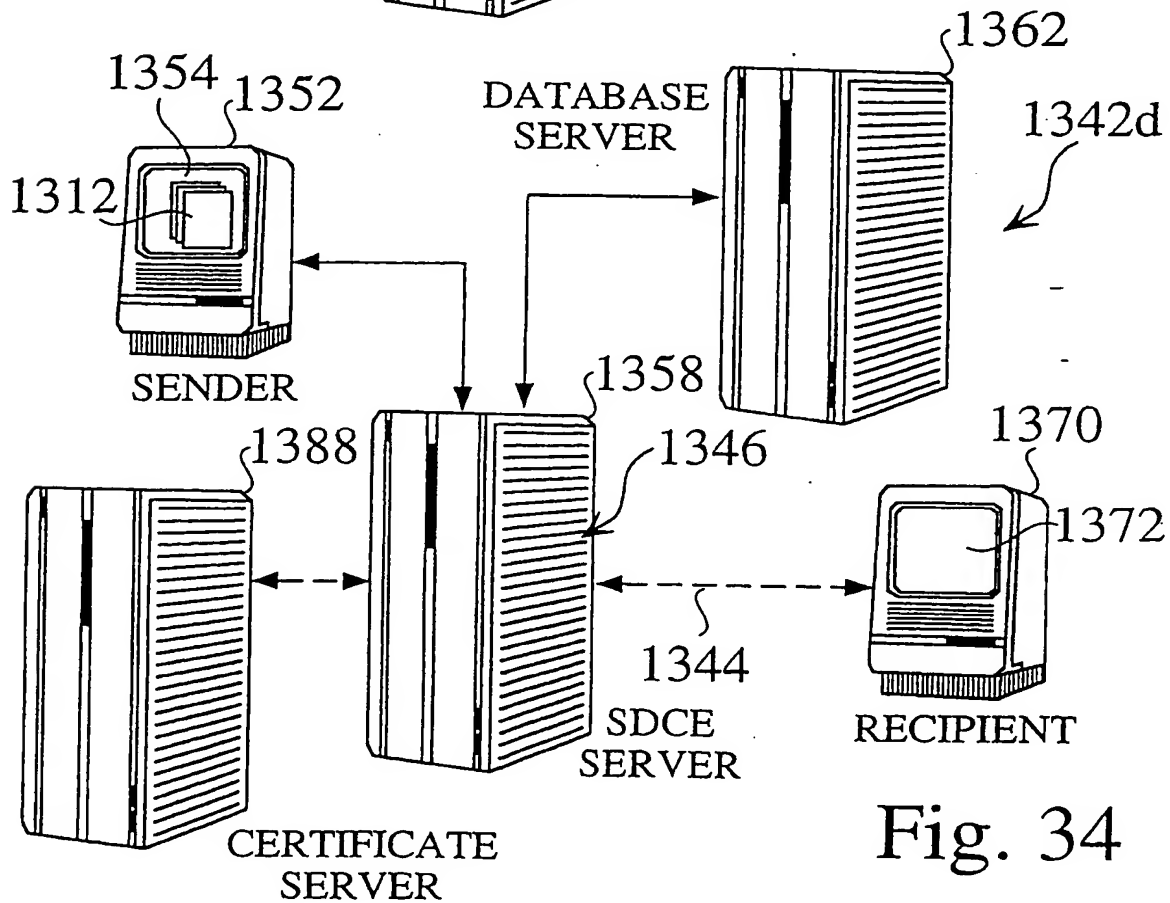


Fig. 34

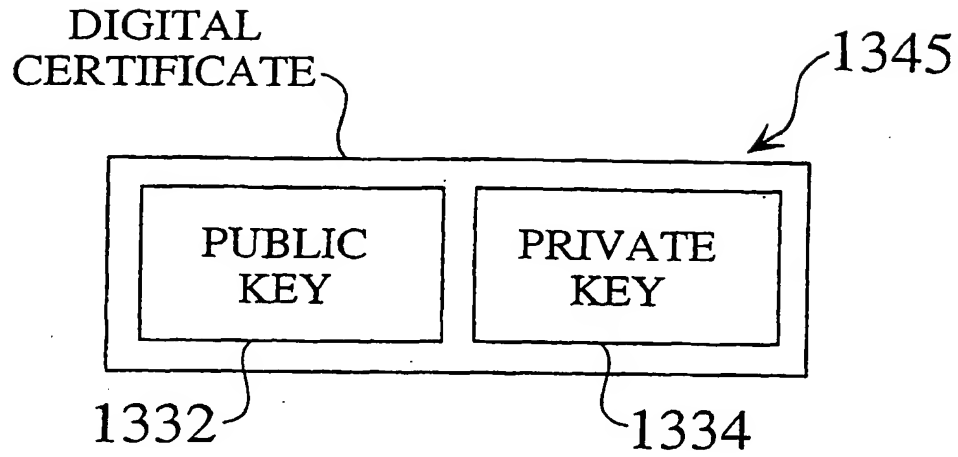


Fig. 35

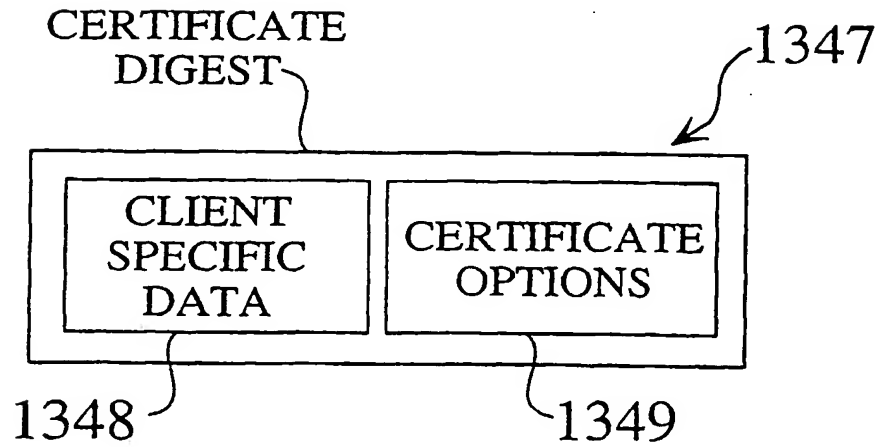


Fig. 36

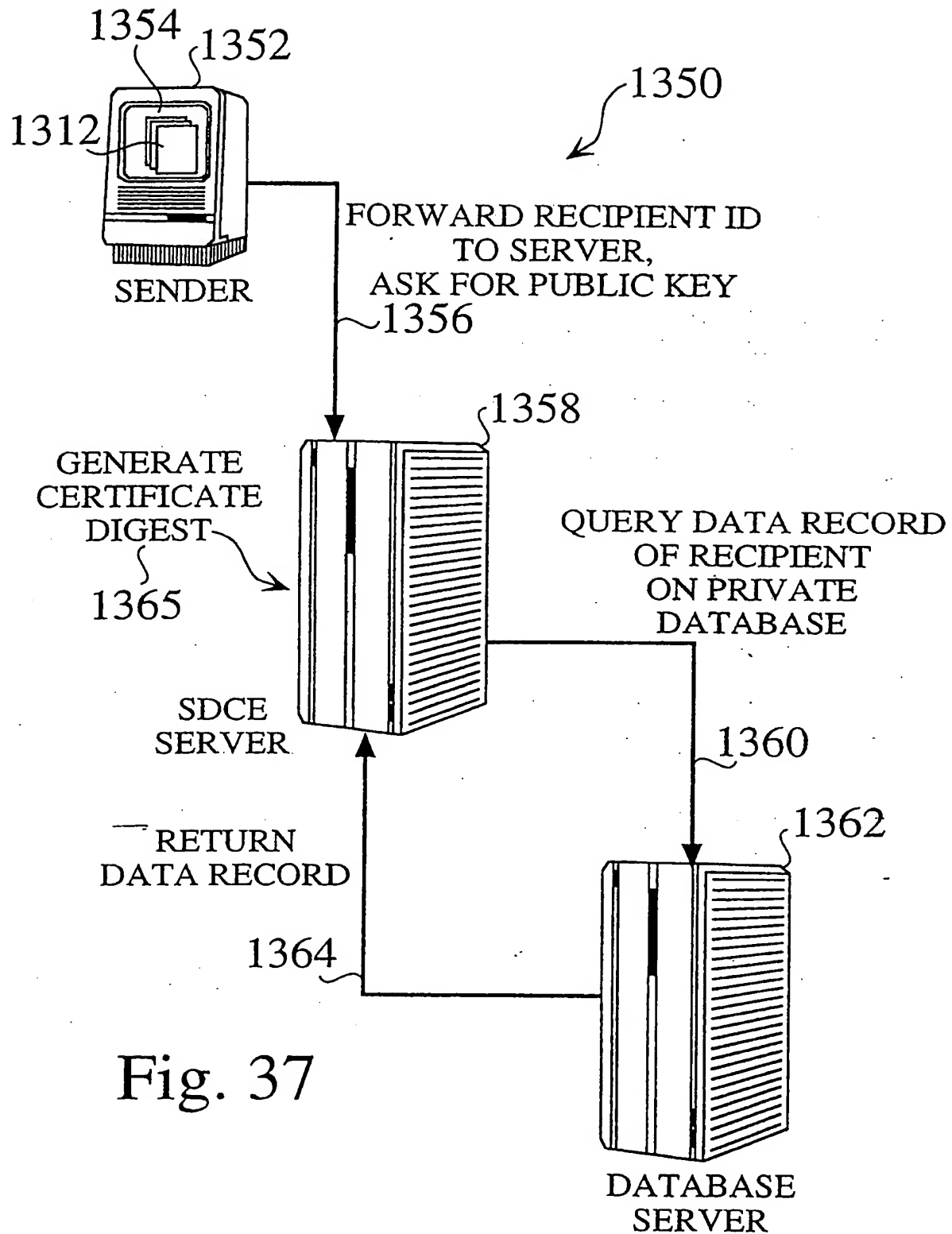


Fig. 37

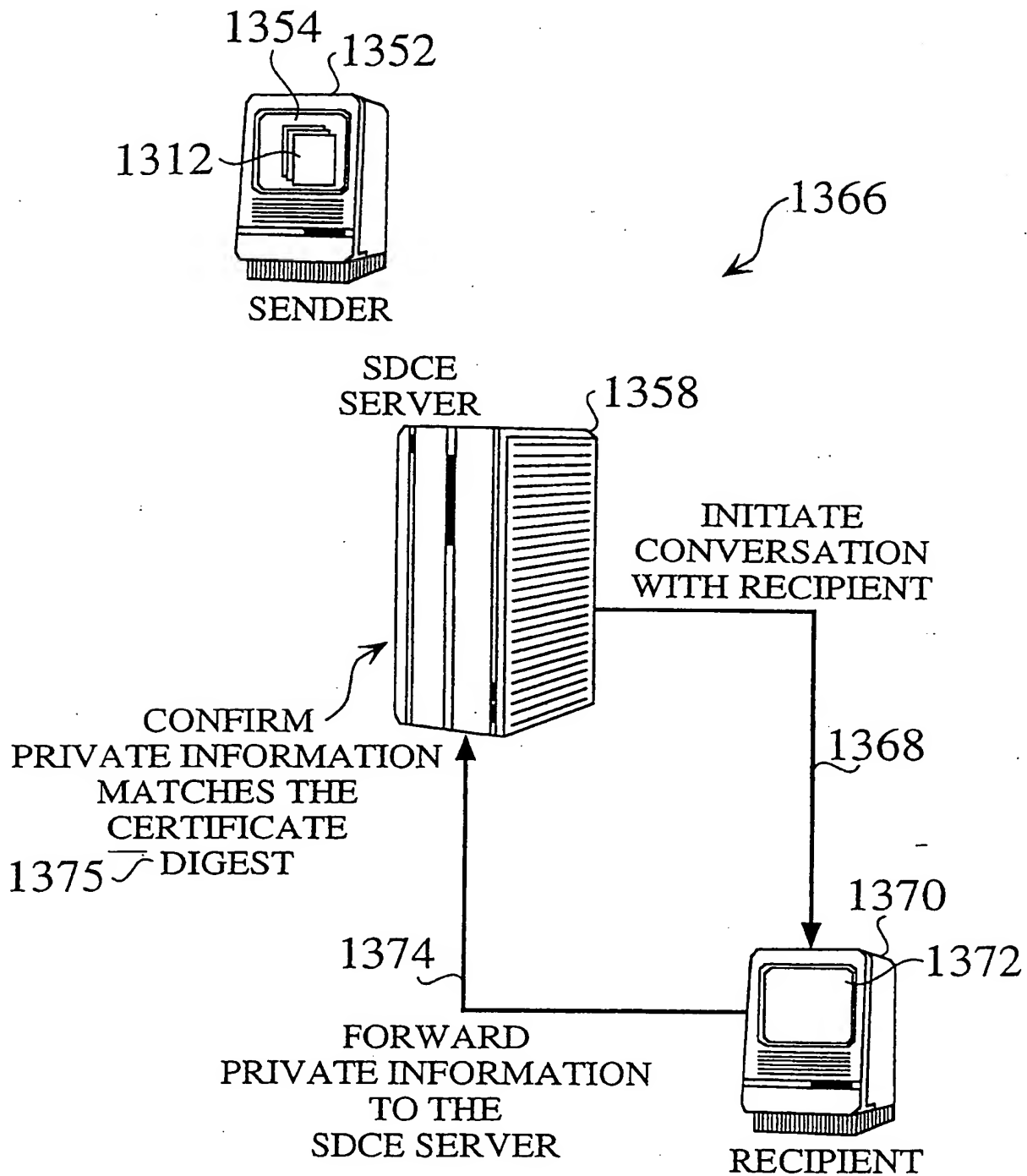


Fig. 38

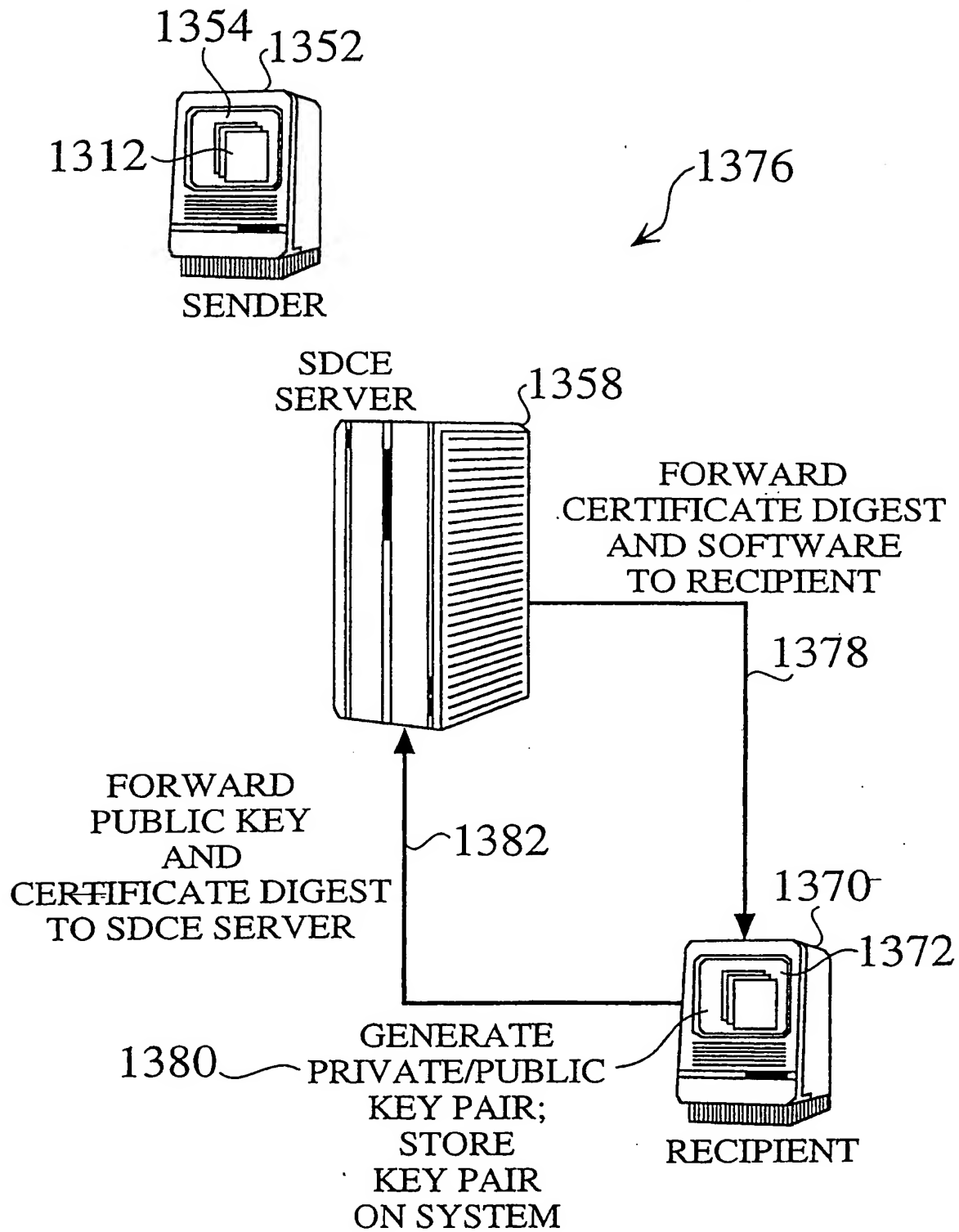


Fig. 39

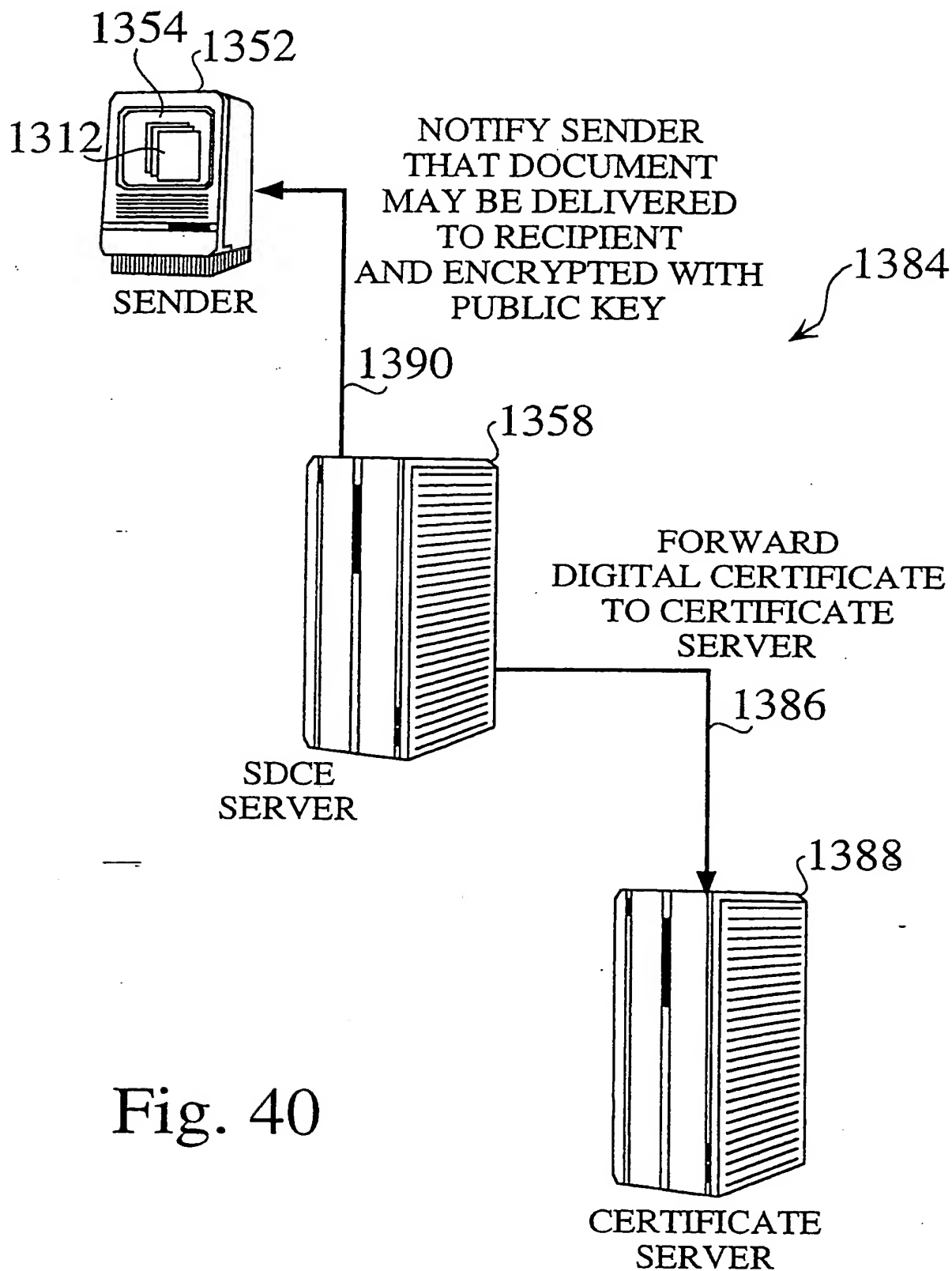


Fig. 40

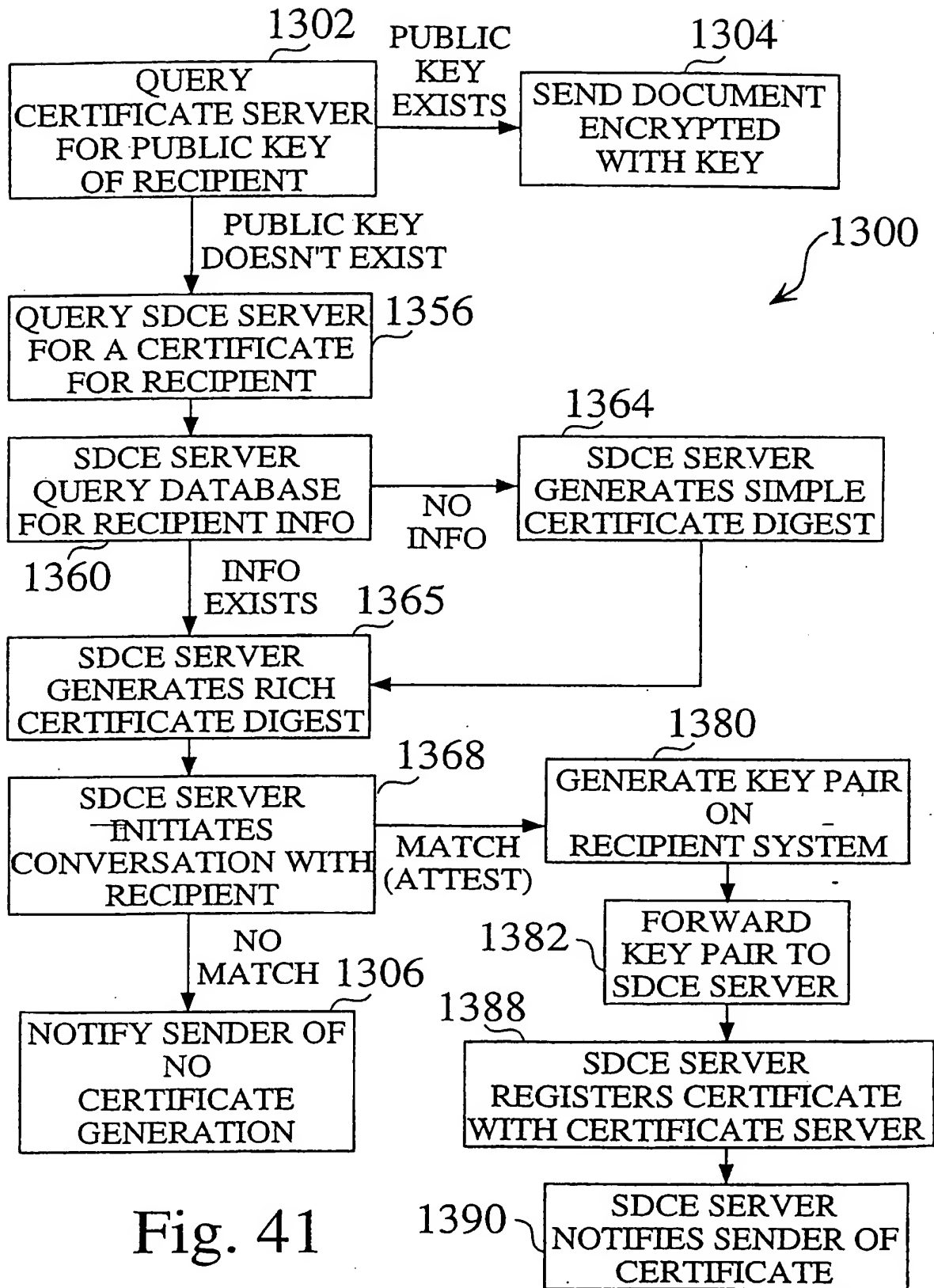


Fig. 41